BENUTZERHANDBUCH

KASPERSKY INTERNET SECURITY 2010

Sehr geehrter Benutzer!

Vielen Dank, dass Sie unser Produkt ausgewählt haben. Wir hoffen, dass diese Dokumentation Ihnen hilft und die meisten Fragen damit beantwortet werden können.

Jedwedes Kopieren, Weiterbreiten oder zum Beispiel Übersetzen von Unterlagen wird nur schriftlich von Kaspersky Lab Ltd. genehmigt.

Das Dokument und dazu gehörenden Grafiken dürfen nur zu informativen, nicht gewerblichen oder persönlichen Zwecken gebraucht werden.

Das Dokument darf ohne vorherige Benachrichtigung geändert werden. Die neueste Version finden Sie auf der Seite von Kaspersky Lab unter der Adresse http://www.kaspersky.com/de/docs.

Für den Inhalt, die Güte, Aktualität und Richtigkeit der im Dokument verwendeten Unterlagen, deren Rechte anderen Rechteinhabern gehören, sowie für den möglichen Schaden durch die Nutzung dieser Unterlagen, lehnt Kaspersky Lab Ltd. die Haftung ab.

In diesem Dokument werden Namen gebraucht, die eingetragene oder nicht eingetragene Warenzeichen sind. Sie gehören den jeweiligen Inhabern.

© Kaspersky Lab, 1997-2009

http://www.kaspersky.de
http://support.kaspersky.de

Redaktionsdatum: 21.05.09

INHALT

EINLEITUNG 11
Lieferumfang 11
Service für registrierte Benutzer 11
Hard- und Softwarevoraussetzungen für das System 12
KASPERSKY INTERNET SECURITY 2010 13
Suche nach Informationen über das Programm 13
Informationsquellen zur selbständigen Recherche 13
Kontaktaufnahme mit der Vertriebsabteilung 14
Kontaktaufnahme mit dem technischen Support 14
Diskussion über die Programme von Kaspersky Lab im Webforum 15
NEUERUNGEN IN KASPERSKY INTERNET SECURITY 2010 16
SCHUTZKONZEPT FÜR IHREN COMPUTER 18
Schutzkomponenten 18
Aufgaben zur Virensuche 20
Update 20
Schutz für Daten und Online-Aktivität 20
Kontrolle über Programme und über den Zugriff auf Daten 21
Assistenten und Werkzeuge 21
Servicefunktionen des Programms 22
KASPERSKY INTERNET SECURITY AUF EINEM COMPUTER INSTALLIEREN 23
Schritt 1. Nach neuer Programmversion suchen 24
Schritt 2. Systemkompatibilität für Installation prüfen 24
Schritt 3. Installationstyp auswählen 25
Schritt 4. Lizenzvereinbarung anzeigen 25
Schritt 5. Erklärung zur Verwendung von Kaspersky Security Network 25
Schritt 6. Installationsverzeichnis auswählen 25
Schritt 7. Programmkomponenten für Installation auswählen 26
Schritt 8. Firewall von Microsoft Windows deaktivieren 26
Schritt 9. Programmeinstellungen einer Vorgängerversion verwenden 27
Schritt 10. Nach anderen Antiviren-Anwendungen suchen 27
Schritt 11. Programminstallation abschließend vorbereiten 28
Schritt 12. Installationsvorgang abschließen 28
ERSTE SCHRITTE 29
Konfigurationsassistent des Programms 30
Schritt 1. Programm aktivieren 30
Schritt 2. Schutzmodus auswählen 32
Schritt 3. Programm-Update anpassen 32
Schritt 4. Kontrolle des Zugriffs auf das Programm 33
Schritt 5. Erkennbare Bedrohungen auswählen 33
Schritt 6. Zwischenspeicherung von Domänennamen (DNS) deaktivieren 33
Schritt 7. Systemanalyse 34
Schritt 8. Assistent abschließen 34
Netzwerktyp auswählen 34
Programm-Update 34

Virenuntersuchung des Computers ... 35
Untersuchung des Computers auf Schwachstellen ... 35
Lizenzverwaltung ... 36
Teilnahme an Kaspersky Security Network ... 36
Sicherheitsverwaltung ... 37
Schutzstatus ... 39
Schutz anhalten ... 40

PROGRAMMOBERFLÄCHE ... 41
Symbol im Infobereich der Taskleiste ... 41
Kontextmenü ... 42
Hauptfenster von Kaspersky Internet Security ... 43
Meldungen ... 46
Programmkonfigurationsfenster ... 46

SCHUTZ FÜR DAS DATEISYSTEM DES COMPUTERS ... 47
Algorithmus für die Arbeit der Komponente ... 48
Sicherheitsstufe für Dateien und Speicher ändern ... 49
Aktion für gefundene Objekte ändern ... 49
Schutzbereich festlegen ... 50
Heuristische Analyse verwenden ... 51
Untersuchung optimieren ... 52
Untersuchung von zusammengesetzten Dateien ... 52
Untersuchung umfangreicher zusammengesetzter Dateien ... 52
Untersuchungsmodus ändern ... 53
Untersuchungstechnologie ... 53
Komponente anhalten: Zeitplan erstellen ... 54
Komponente anhalten: Liste der Programme erstellen ... 55
Standardmäßige Schutzparameter wiederherstellen ... 56

E-MAIL-SCHUTZ ... 57
Algorithmus für die Arbeit der Komponente ... 58
Sicherheitsstufe für den E-Mail-Schutz ändern ... 58
Aktion für gefundene Objekte ändern ... 59
Schutzbereich festlegen ... 60
E-Mail-Untersuchung in Microsoft Office Outlook ... 60
E-Mail-Untersuchung in The Bat! ... 61
Heuristische Analyse verwenden ... 62
Untersuchung von zusammengesetzten Dateien ... 62
Anlagenfilterung ... 62
Standardparameter für den Mail-Schutz wiederherstellen ... 63

SCHUTZ FÜR WEB-DATENVERKEHR ... 64
Algorithmus für die Arbeit der Komponente ... 65
Sicherheitsstufe für den HTTP-Datenverkehr ändern ... 66
Aktion für gefundene Objekte ändern ... 66
Schutzbereich festlegen ... 67
Untersuchungstyp auswählen ... 67
Modul zur Link-Untersuchung ... 68
Heuristische Analyse verwenden ... 69
Untersuchung optimieren ... 69

Standardparameter für den Web-Schutz wiederherstellen ... 70
SCHUTZ FÜR DEN DATENVERKEHR VON INSTANT-MESSENGERN ... 71
Algorithmus für die Arbeit der Komponente ... 72
Schutzbereich festlegen ... 72
Untersuchungsmethode auswählen ... 72
Heuristische Analyse verwenden ... 73
PROGRAMMKONTROLLE ... 74
Algorithmus für die Arbeit der Komponente ... 75
Rechte erben ... 75
Risikobewertung ... 76
Programmgruppen ... 76
Startfolge eines Programms ... 77
Schutzbereich festlegen ... 77
Regeln für die Programmkontrolle ... 79
Programme zu Gruppen zuordnen ... 80
Dauer der Statusermittlung für ein Programm ändern ... 80
Regel für ein Programm ändern ... 81
Regel für eine Programmgruppe ändern ... 81
Netzwerkregel für ein Programm erstellen ... 82
Ausnahmen anpassen ... 82
Regeln für Programme löschen ... 83
SICHERE UMGEBUNG FÜR DIE AUSFÜHRUNG VON PROGRAMMEN ... 84
Start eines Programms in der Sicheren Umgebung ... 85
Verknüpfung für den Start von Programmen erstellen ... 85
Liste der Programme erstellen, die in der Sicheren Umgebung gestartet werden sollen ... 86
Modus auswählen: Programm starten ... 86
Modus auswählen: Daten der Sicheren Umgebung löschen ... 87
Gemeinsamen Ordner verwenden ... 87
Sicheren Umgebung bereinigen ... 88
FIREWALL ... 89
Netzwerkstatus ändern ... 89
Adressenbereich eines Netzwerks erweitern ... 90
Modus für die Benachrichtigung über Veränderungen eines Netzwerks auswählen ... 91
Erweiterte Einstellungen für die Firewall ... 91
Firewall-Regeln ... 92
Paketregel erstellen ... 92
Regel für ein Programm erstellen ... 93
Assistent für neue Regeln ... 94
Aktion auswählen, die von einer Regel ausgeführt werden soll ... 94
Parameter eines Netzwerkdiensts anpassen ... 95
Adressenbereich auswählen ... 95
PROAKTIVER SCHUTZ ... 97
Liste der gefährlichen Aktivität verwenden ... 97
Kontrollregel für gefährliche Aktivität ändern ... 98
Gruppe mit vertrauenswürdigen Programmen erstellen ... 99
Kontrolle über Systembenutzerkonten ... 99

SCHUTZ VOR NETZWERKANGRIFFEN ... 100
Angreifende Computer sperren ... 100
Arten der erkennbaren Netzwerkangriffe ... 100
ANTI-SPAM ... 103
Algorithmus für die Arbeit der Komponente ... 104
Anti-Spam-Training ... 106
Training mit Hilfe des Trainingsassistenten ... 106
Anti-Spam-Training mit ausgehenden E-Mails ... 107
Training mit Hilfe eines Mailprogramms ... 108
Training mit Berichten ... 109
Sicherheitsstufe ändern ... 109
Untersuchungsmethode auswählen ... 110
Liste mit vertrauenswürdigen Adressen erstellen ... 111
Liste mit verbotenen Absendern erstellen ... 111
Liste mit verbotenen Phrasen erstellen ... 112
Liste mit anstößigen Phrasen erstellen ... 112
Liste der erlaubten Absender erstellen ... 113
Liste mit erlaubten Phrasen erstellen ... 114
Liste mit erlaubten Absendern importieren ... 114
Faktor für Spam und potentiellen Spam festlegen ... 115
Algorithmus zur Spam-Erkennung auswählen ... 116
Zusätzliche Merkmale für die Spam-Filterung verwenden ... 116
Markierung zum Betreff einer Nachricht hinzufügen ... 117
Filterung von E-Mails auf dem Server. Mail-Manager ... 117
Nachrichten für Microsoft Exchange Server von der Untersuchung ausschließen ... 118
Aktionen für unerwünschte E-Mails ... 118
Spam-Verarbeitung in Microsoft Office Outlook anpassen ... 119
Spam-Verarbeitung in Microsoft Outlook Express (Windows Mail) anpassen ... 120
Spam-Verarbeitung in The Bat! anpassen ... 121
Spam-Verarbeitung in Thunderbird anpassen ... 122
Standardparameter für Anti-Spam wiederherstellen ... 122
ANTI-BANNER ... 123
Heuristische Analyse verwenden ... 123
Erweiterte Einstellungen für die Komponente ... 124
Liste der erlaubten Banneradressen erstellen ... 124
Liste der verbotenen Banneradressen erstellen ... 125
Bannerlisten exportieren / importieren ... 125
KINDERSICHERUNG ... 126
Algorithmus für die Arbeit der Komponente ... 127
Arbeit mit Profilen ... 128
Profile wechseln ... 128
Beschränkungsniveau ändern ... 129
Beschränkungen für die Anzeige von Webressourcen ... 130
Liste mit erlaubten Webadressen erstellen ... 130
Liste mit verbotenen Webadressen erstellen ... 132
Liste mit Webadressen exportieren / importieren ... 132
Kategorien für verbotene Webadressen auswählen ... 133
Heuristische Analyse verwenden ... 134

Aktion bei einem Zugriffsversuch auf verbotene Webadressen auswählen ... 134
Zeitbeschränkung für den Zugriff ... 134
UNTERSUCHUNG DES COMPUTERS ... 136
Virensuche ... 136
Start der Untersuchungsaufgabe ... 138
Verknüpfung für den Aufgabenstart erstellen ... 139
Liste der Untersuchungsobjekte erstellen ... 139
Sicherheitsstufe ändern ... 140
Aktion beim Fund einer Bedrohung ändern ... 140
Typ der zu untersuchenden Objekte ändern ... 141
Untersuchung optimieren ... 142
Wechseldatenträger untersuchen ... 142
Untersuchung von zusammengesetzten Dateien ... 143
Untersuchungstechnologie ... 144
Untersuchungsmethode ändern ... 144
Startmodus: Zeitplan erstellen ... 145
Startmodus: Benutzerkonto festlegen ... 145
Besonderheiten beim Start von geplanten Untersuchungsaufgaben ... 146
Standardmäßige Untersuchungseinstellungen wiederherstellen ... 146
Suche nach Schwachstellen ... 147
Aufgabe zur Suche nach Schwachstellen starten ... 147
Verknüpfung für den Aufgabenstart erstellen ... 148
Liste der Untersuchungsobjekte erstellen ... 148
Startmodus: Zeitplan erstellen ... 149
Startmodus: Benutzerkonto festlegen ... 150
UPDATE ... 151
Update starten ... 152
Rollback zum vorherigen Update ... 153
Updatequelle auswählen ... 153
Proxyserver verwenden ... 154
Regionsoptionen ... 154
Aktionen nach dem Update ... 154
Update aus einem lokalen Ordner ... 155
Startmodus für die Updateaufgabe ändern ... 156
Updatestart mit den Rechten eines anderen Benutzers ... 156
PROGRAMMPARAMETER ANPASSEN ... 157
Schutz ... 159
Computerschutz aktivieren / deaktivieren ... 159
Kaspersky Internet Security beim Hochfahren des Betriebssystems starten ... 159
Interaktiven Schutzmodus verwenden ... 160
Kontrolle des Zugriffs auf Kaspersky Internet Security ... 160
Datei-Anti-Virus ... 161
Mail-Anti-Virus ... 161
Web-Anti-Virus ... 162
IM-Anti-Virus ... 163
Programmkontrolle ... 163
Firewall ... 164
Proaktiver Schutz ... 165

Schutz vor Netzwerkangriffen ... 165
Anti-Spam ... 166
Anti-Banner ... 167
Kindersicherung ... 168
Untersuchung ... 169
Update ... 170
Einstellungen ... 170
Selbstschutz für Kaspersky Internet Security ... 170
Technologie zur Desinfektion einer aktiven Infektion ... 171
Arbeit von Kaspersky Internet Security auf einem Laptop ... 171
Leistung des Computers beim Ausführen von Aufgaben ... 172
Funktionsparameter für Kaspersky Internet Security exportieren / importieren ... 172
Standardparameter wiederherstellen ... 173
Bedrohungen und Ausnahmen ... 173
Netzwerk ... 177
Meldungen ... 182
Berichte und Speicher ... 183
Feedback ... 187
Aussehen des Programms ... 187
Profile für Kaspersky Internet Security verwenden ... 188

ZUSÄTZLICHE OPTIONEN ... 190
Virtuelle Tastatur ... 190
Kindersicherung ... 191
Notfall-CD ... 191
Notfall-CD erstellen ... 192
Hochfahren eines Computers mit Hilfe der Notfall-CD ... 193
Browser-Konfiguration ... 194
Analyse von Netzwerkpaketen ... 195
Zugriff auf die Analyse von Netzwerkpaketen ... 195
Überwachung von Paketen starten / beenden ... 195
Paketfilterung nach Ursprungs- und Zieladressen ... 196
Paketfilterung nach Übertragungsprotokoll ... 196
Wiederherstellung nach Infektion ... 196
Assistent zum Löschen von Aktivitätsspuren ... 197
Netzwerkmonitor ... 198

BERICHTE ... 199
Komponente oder Aufgabe für das Erstellen eines Berichts auswählen ... 199
Anordnung von Informationen im Bericht ... 200
Über Bereitschaft des Berichts benachrichtigen ... 200
Ereignistyp auswählen ... 201
Darstellung von Daten auf dem Bildschirm ... 202
Darstellung der Statistik als Tabelle oder Grafik ... 203
Bericht in Datei speichern ... 204
Verwendung der komplexen Filterung ... 204
Suche nach Ereignissen ... 205

MELDUNGEN ... 207
Verdächtiges Objekt wurde gefunden ... 208
Desinfektion des Objekts ist nicht möglich ... 209

Spezielle Desinfektionsprozedur ist erforderlich ... 209
Gefährliches Objekt wurde im Datenstrom gefunden ... 210
Verdächtiges Objekt wurde gefunden ... 210
Gefährliche Aktivität im System wurde erkannt ... 211
Versteckter Prozess wurde gefunden ... 212
Versuch zum Zugriff auf die Systemregistrierung wurde erkannt ... 212
Netzwerkaktivität eines Programms wurde erkannt ... 213
Neues Netzwerk wurde gefunden ... 214
Phishing-Angriff wurde erkannt ... 214
Verdächtiger Link wurde gefunden ... 214
Ein inkorrektes Zertifikat wurde gefunden ... 215

EINSTELLUNGEN VON KASPERSKY INTERNET SECURITY AUF KORREKTHEIT PRÜFEN ... 216
EICAR-"Testvirus" und seine Modifikationen ... 216
Testen des Schutzes für HTTP-Datenverkehr ... 218
Schutz für den SMTP-Datenverkehr testen ... 218
Überprüfung der Einstellungen von Datei-Anti-Virus ... 218
Überprüfung der Einstellungen für eine Aufgabe zur Virensuche ... 219
Überprüfung der Einstellungen für den Schutz vor unerwünschten E-Mails ... 219

BEDIENUNG DES PROGRAMMS ÜBER DIE BEFEHLSZEILE ... 220
Programm aktivieren ... 221
Steuerung von Komponenten und Aufgaben des Programms ... 222
Virensuche ... 224
Programm-Update ... 227
Rollback zum vorherigen Update ... 227
Schutzparameter exportieren ... 228
Schutzparameter importieren ... 228
Programm starten ... 229
Programm beenden ... 229
Protokolldatei anlegen ... 229
Hilfe anzeigen ... 230
Rückgabecodes der Befehlszeile ... 230

PROBLEME BEHEBEN ... 231
Bericht über den Systemzustand erstellen ... 231
Protokolldatei erstellen ... 232
Dateien mit Daten senden ... 232
AVZ-Skript ausführen ... 233

ERKLÄRUNG ZUR VERWENDUNG VON KASPERSKY SECURITY NETWORK ... 235

VERWENDUNG DES CODES VON DRITTHERSTELLERN ... 239
CryptoEx Ltd. ... 240
Bibliothek fastscript 1.9 ... 240
Bibliothek pcre 7.4, 7.7 ... 240
Bibliothek GNU bison parser ... 241
Bibliothek AGG 2.4 ... 241
Bibliothek OpenSSL 0.9.8d ... 241
Bibliothek Gecko SDK 1.8 ... 243
Bibliothek zlib 1.2 ... 243
Bibliothek libpng 01.02.08, 01.02.029 ... 243

Bibliothek libnkfm 2.0.5 ... 243
Bibliothek expat 1.2, 2.0.1 ... 243
Bibliothek Info-ZIP 5.51 ... 244
Bibliothek Windows Installer XML (WiX) 2.0 ... 244
Bibliothek passthru ... 247
Bibliothek filter ... 247
Bibliothek netcfg ... 247
Bibliothek pcre 3.0 ... 247
Bibliothek RFC1321-based (RSA-free) MD5 library ... 248
Bibliothek Windows Template Library (WTL 7.5) ... 248
Bibliothek libjpeg 6b ... 251
Bilbiothek libungif 3.0 ... 252
Bibliothek libxdr ... 252
Bibliothek tiniconv - 1.0.0 ... 253
Bibliothek bzip2/libbzip2 1.0.5 ... 257
Bibliothek libspf2-1.2.9 ... 258
Bibliothek Protocol Buffer ... 258
GLOSSAR ... 260
ENDBENUTZER-LIZENZVERTRAG FÜR DIE ERWORBENE KASPERSKY LAB SOFTWARE ... 269
KASPERSKY LAB ... 275
SACHREGISTER ... 276

EINLEITUNG

IN DIESEM ABSCHNITT

Lieferumfang 11

Service für registrierte Benutzer 11

Hard- und Softwarevoraussetzungen für das System 12

LIEFERUMFANG

Sie können Kaspersky Internet Security bei unseren Fachhändlern (als Box mit CD) sowie im Online-Shop kaufen http://www.kaspersky.de.

Haben Sie das Programm in einer Box erworben, gehören zum Lieferumfang des Programms:

- Installations-CD, auf der die Programmdateien und die Dokumentation im PDF-Format gespeichert sind.
- Gedrucktes Benutzerhandbuch und eine Quick-Start-Anleitung(nicht bei allen Box-Typen enthalten).
- Lizenzvereinbarung.
- Aktivierungskarte mit Aktivierungscode und Anleitung zur Aktivierung des Programms.

Die Lizenzvereinbarung ist ein juristischer Vertrag zwischen Ihnen und Kaspersky Lab, in dem steht, unter welchen Bedingungen Sie das von Ihnen gekaufte Programm gebrauchen dürfen.

Lesen Sie sich die Lizenzvereinbarung genau durch!

Wenn Sie die Bedingungen der Lizenzvereinbarung nicht annehmen, können Sie die Box an den Fachhändler zurückgeben, bei dem Sie sie gekauft haben, und Sie bekommen Ihr Geld zurück.

Bevor Sie das Programm installieren, lesen Sie sich bitte die Lizenzvereinbarung sorgfältig durch.

Beim Kauf von Kaspersky Internet Security im Online-Shop kopieren Sie das Programm sowie dieses Handbuch von der Webseite von Kaspersky Lab. Der Aktivierungscode wird Ihnen per E-Mail nach Eingang des Rechnungsbetrages zugestellt.

SERVICE FÜR REGISTRIERTE BENUTZER

Wenn Sie eine Lizenz erwerben, werden Sie ein registrierter Benutzer und während der Gültigkeitsdauer der Lizenz können Sie folgende Leistungen in Anspruch nehmen:

- Stündliche Updates der Programm-Datenbanken und kostenlose Upgrades neuer Programmversionen;
- Beratung bei Fragen zur Installation, Konfiguration und Nutzung des Programms per Telefon und E-Mail;
- Benachrichtigung über neue Versionen und neu aufgetauchte Viren. Dieser Service wird Benutzern geboten, die den Newsletter von Kaspersky Lab auf der Webseite des technischen Supports (http://support.kaspersky.de/subscribe/) abonniert haben.

Der technische Support kann leider keine Fragen zu Funktion und Gebrauch von Betriebssystemen, zu Programmen von Dritten sowie zu verschiedenen Technologien beantworten.

HARD- UND SOFTWAREVORAUSSETZUNGEN FÜR DAS SYSTEM

Um die normale Funktionsfähigkeit von Kaspersky Internet Security 2010 zu gewährleisten, sind folgende Systemvoraussetzungen zu erfüllen:

Allgemeine Anforderungen:

- 300 MB freier Speicherplatz auf der Festplatte
- CD-ROM-Laufwerk (für die Installation von Kaspersky Internet Security 2010 von Installations-CD)
- Microsoft Internet Explorer 6.0 oder höher (für Updates der Datenbanken und Programm-Module über das Internet)
- Microsoft Windows Installer 2.0

➡ *Microsoft Windows XP Home Edition (Service Pack 2),* Microsoft Windows XP Professional (Service Pack 2), Microsoft Windows XP Professional x64 Edition*:*

- Intel Pentium 300 MHz oder höher (oder kompatibel)
- 256 MB Arbeitsspeicher

➡ *Microsoft Windows Vista Home Basic, Microsoft Windows Vista Home Premium, Microsoft Windows Vista Business, Microsoft Windows Vista Enterprise, Microsoft Windows Vista Ultimate:*

- Intel Pentium 800 MHz 32-bit (x86)/ 64-bit (x64) oder höher (oder kompatibel)
- 512 MB Arbeitsspeicher

KASPERSKY INTERNET SECURITY 2010

Kaspersky Internet Security 2010 ist eine neue Generation von Schutzprogrammen.

Der Hauptunterschied zwischen Kaspersky Internet Security 2010 und den restlichen Produkten von Kaspersky Lab, besteht in den komplexen Methoden zum Schutz der Daten auf einem Computer.

IN DIESEM ABSCHNITT

Suche nach Informationen über das Programm 13

SUCHE NACH INFORMATIONEN ÜBER DAS PROGRAMM

Wenn Sie Fragen zu Auswahl, Kauf, Installation oder Verwendung von Kaspersky Internet Security haben, können Sie schnell eine Antwort darauf erhalten.

Kaspersky Lab bietet unterschiedliche Informationsquellen zu dem Programm an. Sie können abhängig von der Dringlichkeit und Bedeutung Ihrer Frage unter diesen Quellen wählen.

IN DIESEM ABSCHNITT

Informationsquellen zur selbständigen Recherche 13

Kontaktaufnahme mit der Vertriebsabteilung 14

Kontaktaufnahme mit dem Technischen Support 14

Diskussion über die Programme von Kaspersky Lab im Webforum 15

INFORMATIONSQUELLEN ZUR SELBSTÄNDIGEN RECHERCHE

Bei Fragen über die Anwendung stehen folgende Informationsquellen zur Verfügung:

Seite auf der Webseite von Kaspersky Lab.

http://www.kaspersky.com/de/kaspersky_internet_security

Auf dieser Seite finden Sie allgemeine Informationen über das Programm, seine Funktionen und Besonderheiten.

Webseite des technischen Supports (Wissensdatenbank)

http://support.kaspersky.com/de/kis2010

Auf dieser Seite finden Sie Artikel, die von Spezialisten des technischen Supports veröffentlicht wurden.

Diese Artikel bieten nützliche Informationen, Tipps und Antworten auf häufige Fragen zu Kauf, Installation und Verwendung der Programme von Kaspersky Lab. Die Artikel können auch Fragen behandeln, die neben diesem Programm auch andere Produkte von Kaspersky Lab betreffen. Außerdem können sie allgemeine Neuigkeiten über den technischen Support enthalten.

Interaktiver Support

Auf der Seite dieses Dienstes finden Sie eine regelmäßig aktualisierte Datenbank von häufig gestellten Fragen und Antworten. Um diesen Dienst nutzen zu können, ist eine Internetverbindung erforderlich.

Um zur Seite für diesen Dienst zu wechseln, klicken Sie im Programmhauptfenster auf den Link **Support** und im folgenden Fenster auf die Schaltfläche **Interaktiver Support**.

Elektronisches Hilfesystem

Im Lieferumfang des Programms ist eine vollständige und kontextorientierte Hilfedatei enthalten. Sie bietet Informationen zu folgenden Aspekten der Verwaltung des Computerschutzes: Anzeige des Schutzstatus, Untersuchung bestimmter Computerbereiche auf Viren, Ausführen anderer Aufgaben, sowie Informationen zu jedem Fenster der Anwendung: Liste und Beschreibung der in einem Fenster vorhandenen Parameter und Liste der ausführbaren Aufgaben.

Um die Hilfe zu öffnen, klicken Sie im entsprechenden Fenster auf die Schaltfläche **Hilfe** oder auf die Taste **<F1>**.

Dokumentation

Zum Lieferumfang von Kaspersky Internet Security gehört das **Benutzerhandbuch** (im PDF-Format). Es enthält eine ausführliche Beschreibung aller Funktionen.

KONTAKTAUFNAHME MIT DER VERTRIEBSABTEILUNG

Bei Fragen zur Auswahl oder zum Kauf von Kaspersky Internet Security sowie zur Verlängerung der Nutzungsdauer stehen Ihnen die Mitarbeiter der Vertriebsabteilung unter folgenden Rufnummern zur Verfügung:

+49 (0)841 – 981 89 560

Sie können sich mit Ihrer Frage auch unter folgender Adresse per E-Mail an die Mitarbeiter der Vertriebsabteilung wenden: vertrieb@kaspersky.de.

KONTAKTAUFNAHME MIT DEM TECHNISCHEN SUPPORT

Als Besitzer einer Lizenz von Kaspersky Internet Security, können Sie von den Spezialisten des technischen Supports per Telefon oder über das Internet Hilfe erhalten.

Die Spezialisten des technischen Supports beantworten Ihre Fragen zur Installation und Verwendung des Programms und helfen Ihnen dabei, die Folgen von Virenangriffen zu beheben, wenn Ihr Computer infiziert wurde.

Bevor Sie sich an den technischen Support wenden, lesen Sie sich bitte zuvor die Supportrichtlinien (http://support.kaspersky.com/de/support/rules) durch.

E-Mail-Anfrage an den technischen Support

Die Support-Spezialisten werden Ihre Frage per E-Mail an die in der Anfrage angegebene Adresse beantworten.

Beschreiben Sie im Webformular das aufgetretene Problem möglichst genau. Machen Sie in den obligatorisch auszufüllenden Feldern folgende Angaben:

- **Typ der Anfrage**. Wählen Sie die Problemart aus, dem Ihr Problem möglichst nahe kommt.
- **Name und Versionsnummer des Programms**.
- **Anfragetext**. Beschreiben Sie das Problem möglichst genau.
- **E-Mail-Adresse**. An diese Adresse werden die Support-Spezialisten Ihre Anfrage beantworten.

Technischer Support am Telefon

Zur Lösung dringender Probleme können Sie den lokalen technischen Support anrufen. Informationen hierzu finden Sie unter www.kaspersky.de/technischer_support

DISKUSSION ÜBER DIE PROGRAMME VON KASPERSKY LAB IM WEBFORUM

Wenn Ihre Frage keine dringende Antwort erfordert, können Sie sie mit den Spezialisten von Kaspersky Lab und mit anderen Anwendern in unserem Forum unter der Adresse http://forum.kaspersky.com diskutieren.

Im Forum können Sie bereits veröffentlichte Themen nachlesen, eigene Beiträge schreiben, neue Themen eröffnen und die Hilfefunktion verwenden.

NEUERUNGEN IN KASPERSKY INTERNET SECURITY 2010

Kaspersky Internet Security 2010 ist ein universelles Programm für den Informationsschutz. Das Programm schützt nicht nur vor Viren, sondern auch vor Spam und Netzwerkangriffen. Die Programmkomponenten können den Computer außerdem vor unbekannten Bedrohungen und vor Internetbetrug schützen, sowie den Internetzugriff der Computerbenutzer kontrollieren.

Der komplexe Schutz wird auf allen Kanälen gewährleistet, auf denen Daten eingehen und übertragen werden. Flexible Einstellungsmöglichkeiten für alle Komponenten erlauben es, Kaspersky Internet Security präzise an die Erfordernisse eines konkreten Benutzers anzupassen.

Ausführliche Beschreibung der Neuerungen in Kaspersky Internet Security 2010

Neuerungen im Schutz:

- Kaspersky Internet Security enthält nun die Komponente Programmkontrolle (s. S. 74), die zusammen mit dem Proaktiven Schutz und der Firewall einen universellen Schutz vor beliebigen Bedrohungen gewährleistet. Die Komponente registriert die Aktionen, die von Programmen im System ausgeführt werden können, und reguliert in Abhängigkeit von der ihnen zugewiesenen Zuverlässigkeitsstufe, ihre Aktivität. Die Komponente kontrolliert den Zugriff auf persönliche Benutzerdaten sowie auf Parameter und Objekte des Betriebssystems, und verhindert die Ausführung systemgefährlicher Aktionen durch Programme.

- Die neue Komponente IM-Anti-Virus (s. S. 71) gewährleistet Sicherheit bei der Arbeit mit den meisten Instant Messengern. Die Komponente untersucht Nachrichten auf das Vorhandensein gefährlicher Objekte.

- Programme von Drittherstellern können nun in einer geschützten virtuellen Umgebung gestartet werden. Diese heißt „Sichere Umgebung“ (s. S. 84). Der Start von Internetbrowsern in der Sicheren Umgebung gewährleistet die gefahrlose Ansicht von Webseiten und schützt den Computer dabei vor dem Eindringen schädlicher Programme (und damit die Benutzerdaten vor unerlaubten Veränderungen oder dem Löschen). Andererseits bietet die Sichere Umgebung die Möglichkeit, alle Objekte zu löschen, die während einer Internetsitzung gesammelt wurden (temporäre Dateien, Cookies, Chronik der besuchten Webseiten usw.).

- Kaspersky Internet Security umfasst ein Modul zur Link-Untersuchung (s. S. 68), das zu der Komponente Web-Anti-Virus gehört. Das Modul untersucht alle Links, die auf einer Webseite vorhanden sind, auf Zugehörigkeit zu verdächtigen und Phishing-Webadressen. Das Modul wird als Plug-in in die Webbrowser Microsoft Internet Explorer und Mozilla Firefox integriert.

- Der Zugriff auf Phishing-Webadressen und der Schutz vor Phishing-Angriffen werden durch die Untersuchung von Links kontrolliert, die in Nachrichten und auf Webseiten enthalten sind. Außerdem werden Zugriffsversuche auf Webseiten mit einer Datenbank für Phishing-Webadressen überwacht. Die Untersuchung auf Phishing-Webadressen ist für Web-Anti-Virus (s. S. 67), IM-Anti-Virus (s. S. 72) und Anti-Spam (s. S. 110) verfügbar.

- Die Liste der Untersuchungsaufgaben wurde um das neue Tool Suche nach Schwachstellen (s. S. 147) erweitert. Es erleichtert die Suche und Neutralisierung von Sicherheitsrisiken und Schwachstellen in den auf Ihrem Computer installierten Programmen und in den Parametern des Betriebssystems.

Neuerungen auf der Programmoberfläche:

- Mit dem Schutz-Center (s. S. 20) haben Sie den Schutz Ihrer: Dateien und persönliche Benutzerdaten, Objekte des Betriebssystems und auf dem Computer installierten Programme unter Kontrolle, ebenso die Arbeit im Netzwerk. Für jeden Aspekt des Schutzes ist eine spezielle Auswahl der Komponenten von Kaspersky Internet Security verantwortlich. Unter Verwendung des Schutz-Centers kann der Benutzer beurteilen, welche Komponente am Schutz einer bestimmten Ressourcenkategorie beteiligt ist, und schnell zu den entsprechenden Einstellungen gelangen.

- Der neue Abschnitt Programmkontrolle (s. S. 21) gewährleistet den schnellen Zugriff auf die Verwaltung von Schutzparametern, die dazu dienen, die Ausführung systemgefährlicher Aktionen durch Programme zu verhindern und den Zugriff auf Ihre persönlichen Daten zu kontrollieren. Außerdem besteht hier die Möglichkeit, Programme in der Sicheren Umgebung zu starten.

- Assistenten und Werkzeuge (s. S. 21), mit denen spezifische Aufgaben im Bezug auf die Computersicherheit gelöst werden können, sind im Abschnitt **Sicherheit+** zusammengefasst.

SCHUTZKONZEPT FÜR IHREN COMPUTER

Kaspersky Internet Security bietet Ihrem Computer Schutz vor bekannten und neuen Bedrohungen, Netzwerkangriffen und Betrugsversuchen, Spam und anderen unerwünschten Daten. Jeder Bedrohungstyp wird von einer bestimmten Programmkomponente verarbeitet. Dieses Schutzkonzept erlaubt es, das Programm flexibel an die Erfordernisse eines Benutzers anzupassen.

Kaspersky Internet Security verfügt über folgende Schutzwerkzeuge:

- Schutzkomponenten (s. S. 18), die die Sicherheit gewährleisten:
  - für Dateien und persönliche Daten.
  - für das System.
  - für die Arbeit in einem Netzwerk.
- Aufgaben zur Virensuche (s. S. 20), mit denen die Virensuche in einzelnen Dateien, Ordnern, Laufwerken oder Bereichen, oder die vollständige Untersuchung des Computers erfolgt.
- Update (s. S. 20), das den aktuellen Zustand der internen Programm-Module sowie der Datenbanken, die für die Suche nach schädlichen Programmen und zum Erkennen von Netzwerkangriffen und Spam-Mails verwendet werden, aufrechterhält.
- Assistenten und Werkzeuge (s. S. 21), die Aufgaben vereinfachen, die im Verlauf von Kaspersky Internet Security auftreten.
- Servicefunktionen (s. S. 22), die Informationen über die Arbeit mit den Programmen bieten und es erlauben, die Programmfunktionalität zu erweitern.

IN DIESEM ABSCHNITT

Schutzkomponenten 18

Aufgaben zur Virensuche 20

Update 20

Schutz für Daten und Online-Aktivität 20

Kontrolle über Programme und über den Zugriff auf Daten 21

Assistenten und Werkzeuge 21

Servicefunktionen des Programms 22

SCHUTZKOMPONENTEN

Der Echtzeitschutz Ihres Computers wird durch folgende Schutzkomponenten gewährleistet:

Datei-Anti-Virus (s. S. 47)

Datei-Anti-Virus kontrolliert das Dateisystem des Computers. Er untersucht auf Ihrem Computer und auf allen angeschlossenen Laufwerken alle Dateien, die geöffnet, gestartet und gespeichert werden. Jeder Zugriff auf eine Datei wird von Kaspersky Internet Security abgefangen und die Datei wird auf die Existenz bekannter Viren

untersucht. Eine Datei wird nur dann zur Arbeit freigegeben, wenn die Datei virenfrei ist oder erfolgreich vom Programm desinfiziert wurde. Wenn die Desinfektion einer Datei aus irgendwelchen Gründen nicht möglich ist, wird sie gelöscht. Dabei wird ihre Kopie im Backup abgelegt oder in der Quarantäne gespeichert.

Mail-Anti-Virus (s. S. 57)

Mail-Anti-Virus untersucht alle ein- und ausgehenden E-Mails auf Ihrem Computer. Er analysiert E-Mails auf die Existenz von Schadprogrammen. Eine E-Mail wird nur dann dem Empfänger zugestellt, wenn sie keine gefährlichen Objekte enthält. Außerdem analysiert die Komponente E-Mails im Hinblick auf Phishing.

Web-Anti-Virus (s. S. 64)

Web-Anti-Virus fängt die Ausführung von Skripts, die sich auf Webseiten befinden, ab und blockiert sie, falls Sie gefährlich sind. Auch der HTTP-Verkehr unterliegt einer strengen Kontrolle. Außerdem analysiert die Komponente Webseiten im Hinblick auf Phishing.

IM-Anti-Virus (s. S. 71)

IM-Anti-Virus sorgt für die Sicherheit bei Instant-Messengern. Sie schützt die Informationen, die über Instant-Messenger-Protokolle auf Ihren Computer gelangen. IM-Anti-Virus gewährleistet Sicherheit bei der Arbeit mit vielen Programmen, die dem Sofortaustausch von Nachrichten dienen.

Programmkontrolle (s. S. 74)

Die Programmkontrolle registriert die Aktionen, die von Programmen im System ausgeführt werden können, und reguliert in Abhängigkeit von der Gruppe, zu der ein Programm gehört, seine Aktivität. Für jede Gruppe von Programmen ist eine Auswahl von Regeln vorgegeben. Diese Regeln steuern den Zugriff von Programmen auf unterschiedliche Ressourcen.

Firewall (s. S. 89)

Die Firewall gewährleistet Sicherheit in lokalen Netzwerken und im Internet. Sie filtert die gesamte Netzwerkaktivität, wozu zwei Arten von Regeln dienen: *Regeln für Programme* und *Paketregeln*.

Proaktiver Schutz (s. S.. 97)

Der Proaktive Schutz erlaubt es, ein neues Schadprogramm zu erkennen, bevor es Schaden anrichten kann. Die Komponente basiert auf der Kontrolle und Analyse des Verhaltens aller auf Ihrem Computer installierten Programme. Aufgrund der auszuführenden Aktionen entscheidet Kaspersky Internet Security, ob ein Programm potentiell gefährlich ist oder nicht. So ist Ihr Computer nicht nur vor bekannten Viren, sondern auch vor neuen, bisher unbekannten Viren geschützt.

Schutz vor Netzwerkangriffen (s. S. 100)

Der Schutz vor Netzwerkangriffen wird beim Hochfahren des Betriebssystems gestartet und überwacht den eingehenden Datenverkehr auf für Netzwerkangriffe charakteristische Aktivität. Wenn ein Angriffsversuch auf Ihren Computer erkannt wird, blockiert Kaspersky Internet Security jede Art von Netzwerkaktivität des angreifenden Computers im Hinblick auf Ihren Computer.

Anti-Spam (s. S. 103)

Anti-Spam wird in Ihr Mailprogramm integriert und kontrolliert alle eingehenden E-Mail auf Spam. Alle E-Mails, die Spam enthalten, werden durch eine spezielle Kopfzeile markiert. Anti-Spam kann zusätzlich für die Spam-Verarbeitung (automatisches Löschen, Verschieben in einen speziellen Ordner, u.a.) eingestellt werden. Außerdem analysiert die Komponente E-Mails im Hinblick auf Phishing

Netzwerkmonitor (s. S. 198)

Diese Komponente dient dazu, in Echtzeit Informationen über die Netzwerkaktivität anzuzeigen.

Anti-Phishing

Komponente, die in Web-Anti-Virus, Anti-Spam und IM-Anti-Virus integriert ist und mit der Webadressen auf ihre Zugehörigkeit zur Liste der Phishing- und verdächtigen Webadressen untersucht werden können.

Anti-Banner (s. S. 123)

Anti-Banner blockiert Werbung, die auf speziellen Bannern platziert ist, die in das Interface von auf Ihrem Computer installierten Programmen integriert sind oder sich im Internet befinden.

Kindersicherung (s. S. 126)

Die Programmkomponente Kindersicherung kontrolliert den Zugriff von Computerbenutzern auf Webressourcen. Die Hauptaufgabe der Kindersicherung besteht darin, den Zugriff auf folgende Ressourcen zu beschränken: Webseiten, die für Erwachsene bestimmt sind oder die Themen wie Pornografie, Waffen, Drogen betreffen oder Grausamkeit, Gewalt usw. provozieren, sowie Webseiten, die Zeitverlust (Chats, Glücksspiel) oder Geldverlust (Online-Shops, Auktionen) verursachen können.

AUFGABEN ZUR VIRENSUCHE

Neben dem Schutz des Computers, ist es sehr wichtig, regelmäßig eine vollständige Virenuntersuchung Ihres Computers durchzuführen. Das ist erforderlich, um die Möglichkeit der Ausbreitung schädlicher Programme auszuschließen, die nicht von den Schutzkomponenten erkannt wurden, weil beispielsweise eine zu niedrige Schutzstufe eingestellt war.

Kaspersky Internet Security verfügt über folgende Aufgaben zur Virensuche:

- **Objekte untersuchen**. Untersuchung von Objekten, die der Benutzer festlegt. Sie können ein beliebiges Objekt des Dateisystems auf dem Computer untersuchen.
- **Vollständige Untersuchung**. Ausführliche Untersuchung des Systems. Standardmäßig werden folgende Objekte untersucht: Systemspeicher, Objekte, die beim Systemstart gestartet werden, Systemwiederherstellung, Mail-Datenbanken, Festplatten, Wechseldatenträger und Netzlaufwerke.
- **Schnelle Untersuchung**. Virenuntersuchung der Objekte, die beim Start des Betriebssystems geladen werden.

UPDATE

Um stets bereit zu sein, Netzwerkangriffe abzuwehren und Viren oder andere gefährliche Programme zu neutralisieren, ist es unerlässlich, Kaspersky Internet Security immer auf dem neusten Stand zu halten. Dazu dient die Komponente **Update**. Sie ist für die Aktualisierung der Datenbanken und Programm-Module verantwortlich, die bei der Arbeit des Programms verwendet werden.

Der Dienst zur Update-Verteilung erlaubt es, die Updates für Datenbanken und Programm-Module, die von den Kaspersky-Lab-Updateservern heruntergeladen wurden, in einem lokalen Ordner zu speichern. Dieser Ordner kann anderen Netzwerkcomputern als Updatequelle dienen, um Datenverkehr einzusparen.

SCHUTZ FÜR DATEN UND ONLINE-AKTIVITÄT

Kaspersky Internet Security schützt die Daten auf Ihrem Computer vor Malware und nicht autorisierten Zugriff. Außerdem gewährleistet das Programm den sicheren Zugriff auf das lokale Netzwerk und auf das Internet.

Die geschützten Objekte lassen sich in drei Gruppen unterteilen:

- Dateien, persönliche Daten, Einstellungen für den Zugriff auf unterschiedliche Ressourcen (Benutzernamen und Kennwörter), Daten über Scheckkarten usw. Am Schutz dieser Objekte sind Datei-Anti-Virus, Programmkontrolle und Proaktiver Schutz beteiligt.
- Auf Ihrem Computer installierte Programme und Objekte des Betriebssystems. Am Schutz dieser Objekte sind Mail-Anti-Virus, Web-Anti-Virus, IM-Anti-Virus, Programmkontrolle, Proaktiver Schutz, Schutz vor Netzwerkangriffen und Anti-Spam beteiligt.

- Arbeit im Netzwerk: Anzeigen von Seiten, Verwendung von Zahlungssystemen, Schutz des Posteingangs vor Spam und Viren usw. Am Schutz dieser Objekte sind Mail-Anti-Virus, Web-Anti-Virus, IM-Anti-Virus, Firewall, Schutz vor Netzwerkangriffen, Anti-Spam, Netzwerkmonitor, Anti-Banner und Kindersicherung beteiligt.

KONTROLLE ÜBER PROGRAMME UND ÜBER DEN ZUGRIFF AUF DATEN

Kaspersky Internet Security verhindert die Ausführung von systemgefährlichen Aktionen durch Programme, kontrolliert den Zugriff auf persönliche Daten und bietet den Start von Programmen in der Sicheren Umgebung. Dazu dienen folgende Werkzeuge:

- **Aktivitätskontrolle für Programme** (s. S. 74). Diese Komponente registriert die Aktionen, die von Programmen im System ausgeführt werden können, und reguliert in Abhängigkeit von der Gruppe, zu der ein Programm gehört, seine Aktivität. Für jede Gruppe von Programmen ist eine Auswahl von Regeln vorgegeben. Diese Regeln steuern den Zugriff von Programmen auf unterschiedliche Ressourcen.

- **Schutz für persönliche Daten** (s. S. 77). Die Programmkontrolle verwaltet die Rechte von Programmen, die für das Ausführen von Aktionen mit persönlichen Benutzerdaten gelten. Dazu zählen Dateien, Ordner und Registrierungsschlüssel, die Funktionsparameter und wichtige Daten für häufig verwendete Programme enthalten, sowie Dateien des Benutzers (Ordner Eigene Dateien, Cookies-Dateien, Daten über die Benutzeraktivität).

- **Sichere Umgebung für die Ausführung von Programmen** (s. S. 84). Kaspersky Internet Security bietet maximale Sicherheit für Objekte des Betriebssystems und für persönliche Daten. Dazu werden Programme von Drittherstellern in einer sicheren virtuellen Umgebung gestartet.

ASSISTENTEN UND WERKZEUGE

Es ist eine schwierige Aufgabe, die Sicherheit eines Computers zu gewährleisten. Dafür sind Kenntnisse über Besonderheiten der Funktion eines Betriebssystems und über potentielle Schwachstellen erforderlich. Zudem erschweren die große Menge und die Vielfalt der Informationen über die Systemsicherheit deren Analyse und Verarbeitung.

Um spezifische Aufgaben, die die Sicherheit des Computers gewährleisten, zu vereinfachen, verfügt Kaspersky Internet Security über unterschiedliche Assistenten und Werkzeuge.

- Der Assistent zur Browser-Konfiguration (s. S. 194) führt eine Analyse der Einstellungen des Browsers Microsoft Internet Explorer aus. Dabei werden die Einstellungen hauptsächlich im Hinblick auf die Sicherheit bewertet.

- Der Assistent zur Wiederherstellung nach einer Infektion (s. S. 196) beseitigt im System die Spuren von schädlichen Objekten.

- Assistent zum Löschen von Aktivitätsspuren (s. S. 197), der nach Aktivitätsspuren des Benutzers im System und Einstellungen des Betriebssystems sucht und beseitigt, die Daten über die Aktivität des Benutzers sammeln.

- Die Notfall-CD (s. S. 191) dient zur Untersuchung und Desinfektion infizierter x86-kompatibler Computer. Sie kommt dann zum Einsatz, wenn der Infektionsgrad so hoch ist, dass die Desinfektion eines Computers nicht mehr mit Hilfe von Antiviren-Anwendungen oder Desinfektionstools möglich ist.

- Suche nach Schwachstellen (s. S. 147) diagnostiziert die Sicherheit des Computers und sucht nach Schwachstellen im Betriebssystem und in Programmen, die auf dem Computer installiert sind.

- Die Analyse von Netzwerkpaketen (s. S. 195) fängt Netzwerkpakete ab und bietet ausführliche Informationen darüber.

- Der Netzwerkmonitor (s. S. 198) dient dazu, ausführliche Informationen über die Netzwerkaktivität auf Ihrem Computer anzuzeigen.

- Virtuelle Tastatur (s. S. 190), sodass keine über die Tastatur eingegebenen Daten erfasst werden können.

SERVICEFUNKTIONEN DES PROGRAMMS

Kaspersky Internet Security verfügt über folgende Servicefunktionen: Sie dienen dazu, den aktuellen Zustand des Programms aufrechtzuerhalten, die Optionen des Programms zu erweitern und bei der Arbeit Hilfe zu leisten.

Datenverwaltung und Berichte

Im Programmverlauf wird für jede Schutzkomponente, jede Untersuchungs- oder Updateaufgabe des Programms ein Bericht erstellt. Er enthält Informationen über die ausgeführten Operationen und die Arbeitsergebnisse. Dadurch können Sie jederzeit Details über die Arbeit einer beliebigen Komponente von Kaspersky Internet Security nachlesen. Sollten Probleme auftreten, dann können Sie die Berichte an Kaspersky Lab schicken, damit unsere Experten die Situation analysieren und Ihnen möglichst schnell helfen können.

Alle im Hinblick auf die Sicherheit verdächtigen Objekte werden von Kaspersky Internet Security in den speziellen Speicher *Quarantäne* verschoben. Sie werden dort in verschlüsselter Form gespeichert, um eine Infektion des Computers auszuschließen. Sie können die Quarantäneobjekte auf Viren untersuchen, am ursprünglichen Ort wiederherstellen oder löschen. Außerdem können Sie verdächtige Objekte manuell in die Quarantäne verschieben. Alle Objekte, die sich aufgrund der Untersuchung als virenfrei erweisen, werden automatisch am ursprünglichen Ort wiederhergestellt.

Im *Backup* werden Kopien von Objekten gespeichert, die von Kaspersky Internet Security desinfiziert und gelöscht wurden. Diese Kopien werden angelegt, um bei Bedarf die Objekte oder ein Bild der Infektion wiederherzustellen. Auch die Sicherungskopien der Objekte werden in verschlüsselter Form gespeichert, um eine Infektion des Computers auszuschließen.

Sie können ein Objekt aus dem Backup am ursprünglichen Ort wiederherstellen oder die Sicherungskopie löschen.

Lizenz

Beim Kauf von Kaspersky Internet Security wird zwischen Ihnen und Kaspersky Lab ein Lizenzvertrag abgeschlossen, auf dessen Grundlage Sie die Anwendung verwenden dürfen und für einen festgelegten Zeitraum Zugriff auf Updates für die Programm-Datenbanken und auf den technischen Support erhalten. Die Nutzungsdauer sowie andere Informationen, die für die vollfunktionale Arbeit der Anwendung erforderlich sind, sind in der Lizenz angegeben.

Mit der Funktion **Lizenz** können Sie ausführliche Informationen über die von Ihnen verwendete Lizenz erhalten. Außerdem können Sie damit eine neue Lizenz erwerben oder die Gültigkeit der aktiven Lizenz verlängern.

Support

Alle registrierten Benutzer von Kaspersky Internet Security können den technischen Support-Service in Anspruch nehmen. Um die Bedingungen für die Inanspruchnahme zu erfahren, nutzen Sie die Funktion **Support**.

Mit Hilfe der entsprechenden Links gelangen Sie zum Benutzerforum für die Kaspersky-Lab-Produkte oder können auf der Support-Webseite ein Formular mit einer Fehlermeldung oder Rückmeldung über die Arbeit des Programms senden.

Außerdem stehen Ihnen folgende Support-Möglichkeiten zur Verfügung: Technischer Online-Support, Dienste des Kaspersky Accounts und telefonische Beratung durch unsere Fachleute, die Ihnen immer gern beim Umgang mit Kaspersky Internet Security helfen.

KASPERSKY INTERNET SECURITY AUF EINEM COMPUTER INSTALLIEREN

Kaspersky Internet Security wird auf dem Computer interaktiv mit einem Installationsassistenten installiert.

Vor der Installation sollten Sie alle laufenden Programme schließen.

Um Kaspersky Internet Security auf Ihrem Computer zu installieren, starten Sie auf der CD-ROM mit dem Programm die ausführbare Datei (mit der Endung *.exe).

Der Installationsvorgang für das Programm Kaspersky Internet Security, das aus dem Internet bezogen wurde, ist komplett identisch mit der Installation von der CD-ROM.

Im Anschluss wird nach dem Installationspaket für Kaspersky Internet Security gesucht (Datei mit Endung *.msi) und wenn es vorliegt, wird nach einer neuen Version auf den Kaspersky-Lab-Servern im Internet geprüft. Wenn die Datei des Installationspaketes nicht gefunden wird, wird Ihnen der Download vorgeschlagen. Nach dem Download wird die Installation von Kaspersky Internet Security gestartet. Sollten Sie den Download nicht wünschen, geht die Installation des Programms normal weiter.

Der Installer ist wie ein Assistent. In jedem Fenster stehen verschiedene Schaltflächen, um den Installationsvorgang zu verwalten. Es folgt eine kurze Beschreibung:

- **Weiter** – Vorgang wird angenommen und es geht weiter zum nächsten Schritt im Installationsvorgang.
- **Zurück** – Rückkehr zum vorangegangenen Schritt der Installation.
- **Abbrechen** – Installation wird abgebrochen.
- **Fertig** – Installationsvorgang des Programms auf dem Computer wird beendet.

Es folgt eine detaillierte Beschreibung jedes Schrittes im Installationsvorgang.

IN DIESEM ABSCHNITT

Schritt 1. Nach neuer Programmversion suchen 24

Schritt 2. Systemkompatibilität für Installation prüfen 24

Schritt 3. Installationstyp auswählen 25

Schritt 4. Lizenzvereinbarung anzeigen 25

Schritt 5. Erklärung zur Verwendung von Kaspersky Security Network 25

Schritt 6. Installationsverzeichnis auswählen 25

Schritt 7. Programmkomponenten für Installation auswählen 26

Schritt 8. Firewall von Microsoft Windows deaktivieren 26

Schritt 9. Programmeinstellungen einer Vorgängerversion verwenden 27

Schritt 10. Nach anderen Antiviren-Anwendungen suchen 27

Schritt 11. Programminstallation abschließend vorbereiten 28

Schritt 12. Installationsvorgang abschließen 28

SCHRITT 1. NACH NEUER PROGRAMMVERSION SUCHEN

Vor der Installation wird geprüft, ob neuere Versionen von Kaspersky Internet Security auf den Updateservern von Kaspersky Lab vorhanden sind.

Wenn keine neuere Version des Programms auf den Updateservern von Kaspersky Lab gefunden wurde, wird der Installationsassistent für diese Version gestartet.

Wenn auf den Updateservern eine neuere Version von Kaspersky Internet Security vorgefunden wurde, werden Ihnen Download und Installation vorgeschlagen. Sollten Sie die neuere Version ablehnen, wird der Installationsassistent der laufenden Version gestartet. Sollten Sie die Installation der neueren Version annehmen, werden die Programmdateien auf Ihren Computer kopiert und der Installationsassistent wird automatisch gestartet.

SCHRITT 2. SYSTEMKOMPATIBILITÄT FÜR INSTALLATION PRÜFEN

Vor der Installation von Kaspersky Internet Security auf Ihrem Computer wird die Kompatibilität des Betriebssystems und der Service Packs mit den Softwarevoraussetzungen für die Installation abgeglichen. Außerdem werden die Hardwarevoraussetzungen geprüft sowie die Rechte für die Installation des Programms.

Wenn eine Bedingung nicht eingehalten wird, erscheint auf dem Bildschirm eine entsprechende Meldung. In solchen Fällen sollten vor der Installation des Kaspersky-Lab-Programms die benötigten Service Packs durch Windows Update sowie die nötigen Programme installiert werden.

SCHRITT 3. INSTALLATIONSTYP AUSWÄHLEN

Wenn Ihr System komplett die genannten Voraussetzungen erfüllt, keine neuere Version des Programms auf den Updateservern von Kaspersky Lab gefunden wurde oder Sie die Installation einer neueren Version abgelehnt haben, startet auf Ihrem Computer der Installationsassistent der laufenden Version von Kaspersky Internet Security.

In dieser Phase der Installation können Sie einen passenden Typ für die Installation von Kaspersky Internet Security auswählen:

- *Schnelle Installation*. Bei dieser Variante (das Kontrollkästchen **Benutzerdefinierte Installation** ist deaktiviert) wird das Programm in vollem Umfang mit den von Kaspersky-Lab-Fachleuten empfohlenen Schutzeinstellungen auf Ihrem Computer installiert. Nach der Installation wird der Konfigurationsassistent des Programms (auf S. 30) gestartet.

- *Benutzerdefinierte Installation*. In diesem Fall (das Kontrollkästchen **Benutzerdefinierte Installation** ist aktiviert) können Sie auswählen, welche Programmkomponenten installiert werden sollen und welcher Installationsordner verwendet werden soll. Außerdem können Sie das Programm aktivieren und einen speziellen Assistenten für die Konfiguration verwenden.

Bei der ersten Variante schlägt der Installationsassistent Ihnen vor, zunächst die Lizenzvereinbarung zu lesen und den Gebrauch des Kaspersky Security Network kennen zu lernen. Danach wird das Programm auf Ihrem Computer installiert.

Bei der zweiten Variante müssen Sie in jeder Phase der Installation einige Daten eingeben oder bestätigen.

Zum Fortsetzen der Installation klicken Sie auf die Schaltfläche **Weiter**. Die Installation lässt sich mit der Schaltfläche **Abbrechen** ablehnen.

SCHRITT 4. LIZENZVEREINBARUNG ANZEIGEN

In dieser Phase müssen Sie die Lizenzvereinbarung lesen, die zwischen Ihnen und Kaspersky Lab eingegangen wird.

Lesen Sie sich die Vereinbarung sorgfältig durch und wenn Sie mit allen Punkt einverstanden sind, klicken Sie auf die Schaltfläche **Akzeptieren**. Die Installation des Programms auf Ihrem Computer wird fortgesetzt.

Zum Ablehnen klicken Sie auf die Schaltfläche **Abbrechen**.

SCHRITT 5. ERKLÄRUNG ZUR VERWENDUNG VON KASPERSKY SECURITY NETWORK

Bei diesem Schritt wird Ihnen angeboten, an dem Programm Kaspersky Security Network teilzunehmen. Eine Beteiligung am Programm sieht vor, dass Daten über neue Bedrohungen, die auf Ihrem Computer erkannt wurden, an Kaspersky Lab geschickt werden, außerdem ein einmaliger Identifikator, den Kaspersky Internet Security für Ihren Computer vergibt, sowie Systeminformationen. Es wird dabei garantiert, dass keine persönlichen Daten gesendet werden.

Lesen Sie sich den Text für den Gebrauch von Kaspersky Security Network gründlich durch. Wenn Sie mit allen Punkten einverstanden sind, setzen Sie das Häkchen im Kontrollkästchen **Ich akzeptiere die Teilnahmebedingungen für Kaspersky Security Network**.

Klicken Sie auf **Weiter**. Die Installation wird fortgesetzt.

SCHRITT 6. INSTALLATIONSVERZEICHNIS AUSWÄHLEN

Dieser Schritt des Installationsassistenten ist nur dann verfügbar, wenn eine benutzerdefinierte Installation des Programms (s. Abschnitt "Schritt 3. Installationstyp auswählen" auf S. 25) gewählt wurde.

In dieser Phase der Installation wird Ihnen vorgeschlagen, den Ordner auf Ihrem Computer zu bestimmen, in den Kaspersky Internet Security installiert wird. Standardmäßig gilt folgender Pfad:

- **<Datenträger> \ Program Files \ Kaspersky Lab \ Kaspersky Internet Security 2010** – für 32-bit-Systeme.
- **<Datenträger> \ Program Files (x86) \ Kaspersky Lab \ Kaspersky Internet Security 2010** – für 64-bit-Systeme.

Sie können einen anderen Ordner angeben, indem Sie auf die Schaltfläche **Durchsuchen** klicken und Sie ihn im Standardfenster für die Ordnerauswahl vorgeben oder einen Pfad in das entsprechende Eingabefeld eintragen.

Beachten Sie: Wenn Sie ein komplettes Installationsverzeichnis manuell eingeben, darf es nicht länger als 200 Zeichen sein und keine Sonderzeichen enthalten.

Zum Fortsetzen der Installation klicken Sie auf die Schaltfläche **Weiter**.

SCHRITT 7. PROGRAMMKOMPONENTEN FÜR INSTALLATION AUSWÄHLEN

Dieser Schritt des Installationsassistenten ist nur dann verfügbar, wenn eine benutzerdefinierte Installation des Programms (s. Abschnitt "Schritt 3. Installationstyp auswählen" auf S. 25) gewählt wurde.

Bei der benutzerdefinierten Installation müssen die Komponenten von Kaspersky Internet Security definiert werden, die Sie auf Ihrem Computer installieren wollen. Standardmäßig werden für die Installation alle Komponenten von Kaspersky Internet Security ausgewählt: Schutzkomponenten, Untersuchungs- und Update-Aufgaben.

Um sich entscheiden zu können, welche Komponenten Sie nicht installieren wollen, sehen Sie sich die Kurzinformationen zur jeweiligen Komponente an. Gehen Sie dazu auf die Komponente in der Liste und lesen Sie im unten stehenden Feld den Text. Im Text werden kurz die Funktion der Komponente und der benötigte Speicherplatz auf dem Datenträger beschrieben.

Um die Installation einer Komponente abzulehnen, öffnen Sie das Kontextmenü auf dem Symbol neben dem Namen der Komponente und gehen Sie auf den Punkt **Komponente nicht nehmen**. Beachten Sie, wenn Sie die Installation einer Komponente verwehren, werden Sie vor einer ganzen Reihe von gefährlichen Programmen nicht geschützt.

Um eine Komponente zur Installation auszuwählen, öffnen Sie das Kontextmenü auf dem Symbol neben dem Namen der Komponenten und gehen Sie auf den Punkt **Komponente auf lokaler Festplatte installieren**.

Nachdem die zu installierenden Komponenten bestimmt worden sind, klicken Sie auf die Schaltfläche **Weiter**. Um zur Liste mit den standardmäßig zu installierenden Komponenten zurückzugehen, klicken Sie auf die Schaltfläche **Zurück**.

SCHRITT 8. FIREWALL VON MICROSOFT WINDOWS DEAKTIVIEREN

Dieser Schritt erfolgt nur, wenn Kaspersky Internet Security auf einem Computer installiert wird, auf dem die Firewall von Microsoft Windows aktiviert ist, und wenn die Komponente Firewall zur Installation ausgewählt wurde.

Bei diesem Schritt der Installation von Kaspersky Internet Security wird Ihnen angeboten, die Firewall des Betriebssystems Microsoft Windows zu deaktivieren, weil die zu Kaspersky Internet Security gehörende Komponente Firewall den umfassenden Schutz Ihrer Arbeit im Netzwerk gewährleistet und ein zusätzlicher Schutz durch Mittel des Betriebssystems nicht erforderlich ist.

Wenn Sie die Komponente Firewall als primäres Schutzwerkzeug bei der Arbeit in einem Netzwerk verwenden möchten, klicken Sie auf die Schaltfläche **Weiter**. Die Firewall von Microsoft Windows wird in diesem Fall automatisch deaktiviert.

Wenn Sie Ihren Computer mit Hilfe der Firewall von Microsoft Windows schützen möchten, wählen Sie die Variante **Firewall von Microsoft Windows verwenden**. Die Komponente Firewall von Kaspersky Internet Security wird in diesem Fall zwar installiert. Um bei der Arbeit des Programms Konflikte zu vermeiden, wird sie aber deaktiviert.

SCHRITT 9. PROGRAMMEINSTELLUNGEN EINER VORGÄNGERVERSION VERWENDEN

Auf dieser Etappe können Sie festlegen, ob bei der Arbeit des Programms die Schutzeinstellungen und Programm-Datenbanken einschließlich der Anti-Spam-Datenbanken verwendet werden sollen, wenn solche auf Ihrem Computer bei der Deinstallation einer älteren Version von Kaspersky Internet Security gespeichert wurden.

Es wird detailliert betrachtet, wie sich die oben beschriebenen Optionen nutzen lassen.

Wenn auf Ihrem Computer bereits eine ältere Version (Build) von Kaspersky Internet Security installiert war und bei der Deinstallation die Programm-Datenbanken auf dem Computer gespeichert wurden, können Sie diese in der zu installierenden Version verwenden. Setzen Sie dazu das Häkchen im Kontrollkästchen **Programm-Datenbanken**. Die ursprünglich mitgelieferten Datenbanken werden nicht auf Ihren Computer kopiert.

Um die Schutzparameter zu verwenden, die Sie in der vorherigen Version eingestellt und auf dem Computer gespeichert haben, aktivieren Sie das Kontrollkästchen **Funktionsparameter des Programms**.

Es wird außerdem empfohlen, die Anti-Spam-Datenbanken zu verwenden, wenn diese bei der Deinstallation der vorherigen Programmversion gespeichert wurden. Dadurch wird ein erneutes Training von Anti-Spam überflüssig. Um die bereits von Ihnen erstellten Spam-Datenbanken zu berücksichtigen, aktivieren Sie das Kontrollkästchen **Anti-Spam-Datenbanken**.

SCHRITT 10. NACH ANDEREN ANTIVIREN-ANWENDUNGEN SUCHEN

In dieser Phase wird nach anderen auf Ihrem Computer installierten Antiviren-Produkten gesucht, darunter auch nach Kaspersky-Lab-Programmen, deren gemeinsame Verwendung mit Kaspersky Internet Security zu Konflikten führen könnte.

Beim Erkennen von solchen Programmen auf Ihrem Computer wird die Liste auf dem Bildschirm angezeigt. Ihnen wird deren Deinstallation vorgeschlagen, bevor Sie mit der Installation fortsetzen.

Unter der Liste mit den erkannten Antiviren-Programmen können Sie die Variante Deinstallation – automatisch oder manuell auswählen.

Wenn unter den erkannten Antiviren-Programmen auch ein Kaspersky-Lab-Programm mit der Version 2009 ist, empfehlen wird, bei dessen manueller Deinstallation die Schlüsseldatei dieses Programms zu speichern. Sie können den Schlüssel für das neue Programm weiter verwenden. Außerdem empfehlen wird, die Quarantäne- und Backup-Objekte zu speichern. Kaspersky Internet Security verschiebt sie automatisch in die Quarantäne der neuen Version und sie können damit weiter arbeiten.

Bei der automatischen Deinstallation eines Programms der Version 2009 speichert das Programm die Aktivierungsdaten und sie werden für die Installation der Version 2010 herangezogen.

Zum Fortsetzen der Installation klicken Sie auf die Schaltfläche **Weiter**.

SCHRITT 11. PROGRAMMINSTALLATION ABSCHLIEßEND VORBEREITEN

In dieser Phase wird Ihnen vorgeschlagen, die Vorbereitungen für die Installation von Kaspersky Internet Security auf Ihrem Computer abzuschließen.

Bei der erstmaligen und benutzerdefinierten Installation (s. Abschnitt "Schritt 3. Installationstyp auswählen" auf S. 25) des Programms wird nicht empfohlen, das Kontrollkästchen **Installationsvorgang schützen** zu deaktivieren. Wenn während der Programminstallation ein Fehler auftritt, kann der eingeschaltete Schutz für ein korrektes Rollback der Installation sorgen. Bei einer wiederholten Installation kann das Häkchen im Kontrollkästchen entfernt werden.

Bei einer Remote-Installation des Programms auf dem Computer über *Windows Remote Desktop* wird empfohlen, das Häkchen im Kontrollkästchen **Installationsvorgang schützen** zu entfernen. Wenn das Häkchen im Kontrollkästchen stehen sollte, kann der Installationsvorgang nicht oder nicht richtig ausgeführt werden.

Zum Fortsetzen der Installation klicken Sie auf die Schaltfläche **Weiter**.

Im Verlauf der Installation unterbrechen die Komponenten von Kaspersky Internet Security, die den Datenverkehr im Netzwerk abfangen, die vorhandenen Netzwerkverbindungen. Die Mehrzahl der getrennten Verbindungen wird nach einiger Zeit wiederhergestellt.

SCHRITT 12. INSTALLATIONSVORGANG ABSCHLIEßEN

Im Fenster **Installation abschließen** stehen Angaben über den Abschluss der Installation von Kaspersky Internet Security auf Ihrem Computer.

Im nächsten Schritt wird das Programm so konfiguriert, dass Ihre Daten auf dem Computer maximal geschützt werden. Kaspersky Internet Security lässt sich schnell und richtig mit dem Konfigurationsassistenten (s. Abschnitt "Konfigurationsassistent des Programms" auf S. 30) einstellen.

Klicken Sie auf die Schaltfläche **Weiter**, um zur Konfiguration des Programms zu wechseln.

ERSTE SCHRITTE

Bei der Entwicklung von Kaspersky Internet Security bestand eine der Hauptaufgaben der Kaspersky-Lab-Spezialisten in der optimalen Konfiguration aller Programmeinstellungen. Das verleiht einem Benutzer unabhängig von seiner Erfahrung mit Computern die Möglichkeit, sofort nach der Programminstallation die Sicherheit des Computers zu gewährleisten, ohne sich weiter mit den Einstellungen zu beschäftigen.

Zur Vereinfachung haben wir versucht, die Voreinstellung auf einer einheitlichen Oberfläche des Konfigurationsassistenten des Programms (s. Abschnitt "Konfigurationsassistent des Programms" auf S. 30) zusammenzufassen, der nach dem Installationsvorgang gestartet wird. Mit Unterstützung des Assistenten können Sie Kaspersky Internet Security aktivieren, die Updateparameter anpassen, den Zugriff auf das Programm mit Hilfe eines Kennworts beschränken und andere Einstellungen vornehmen.

Es kann sein, dass Ihr Computer bereits von Schadprogrammen infiziert wurde, bevor Sie Kaspersky Internet Security installiert haben. Um bereits vorhandene Malware zu finden, starten Sie die Untersuchung des Computers.

Durch Aktionen schädlicher Programme und Systemabstürze können die Einstellungen Ihres Computers beschädigt werden. Starten Sie die Aufgabe Suche nach Schwachstellen (s. Abschnitt "Untersuchung des Computers auf Schwachstellen" auf S. 35), um Schwachstellen des installierten Programms und Anomalien in den Systemeinstellungen zu finden.

Die im Lieferumfang enthaltenen Datenbanken können zum Zeitpunkt der Programminstallation veraltet sein. Starten Sie das Programm-Update (sofern das Update nicht mit Hilfe des Konfigurationsassistenten oder sofort nach der Installation automatisch erfolgt ist).

Die Programmkomponente Anti-Spam verwendet einen lernfähigen Algorithmus zum Erkennen unerwünschter E-Mails. Starten Sie den Trainingsassistenten für Anti-Spam (s. Abschnitt "Training mit Hilfe des Trainingsassistenten" auf S. 106), um die Komponente auf die Arbeit mit Ihren E-Mails einzustellen.

Nach den oben beschriebenen Aktionen ist Kaspersky Internet Security zur Arbeit bereit. Verwenden Sie den Assistenten zu Sicherheitsverwaltung (s. Abschnitt "Sicherheitsverwaltung" auf S. 37), um das Schutzniveau Ihres Computers zu beurteilen.

IN DIESEM ABSCHNITT

Konfigurationsassistent des Programms 30

Netzwerktyp auswählen 34

Programm-Update 34

Virenuntersuchung des Computers 35

Untersuchung des Computers auf Schwachstellen 35

Lizenzverwaltung 36

Abonnement zur automatischen Lizenzverlängerung 36

Teilnahme an Kaspersky Security Network 36

Sicherheitsverwaltung 37

Schutzstatus 39

Schutz anhalten 40

KONFIGURATIONSASSISTENT DES PROGRAMMS

Der Konfigurationsassistent für das Programm wird am Ende der Installation gestartet. Seine Aufgabe ist es, Sie bei der ersten Konfiguration der Parameter für Kaspersky Internet Security zu unterstützen und dabei die Besonderheiten der Aufgaben Ihres Computers zu berücksichtigen.

Der Konfigurationsassistent besteht aus einer Folge von Fenstern (Schritten). Zur Navigation zwischen den Fenstern dienen die Schaltfläche **Zurück** und der Link **Weiter**. Der Assistent wird mit Hilfe der Schaltfläche **Abbrechen** abgeschlossen.

DETAILS ZU DEN EINZELNEN SCHRITTE DES ASSISTENTEN

Schritt 1. Programm aktivieren 30

Schritt 2. Schutzmodus auswählen 32

Schritt 3. Programm-Update anpassen 32

Schritt 4. Kontrolle des Zugriffs auf das Programm 33

Schritt 5. Erkennbare Bedrohungen auswählen 33

Schritt 6. Zwischenspeicherung von Domänennamen (DNS) deaktivieren 33

Schritt 7. Systemanalyse 34

Schritt 8. Assistent abschließen 34

SCHRITT 1. PROGRAMM AKTIVIEREN

Bei der Programmaktivierung wird durch die Installation eines Aktivierungscodes eine Lizenz registriert. Auf Grundlage der Lizenz ermittelt das Programm, ob Rechte für die Programmnutzung bestehen und welche Nutzungsdauer dafür gilt.

Der Schlüssel enthält Dienstinformationen, die für die volle Funktionsfähigkeit von Kaspersky Internet Security erforderlich sind, sowie zusätzliche Angaben:

- Informationen über den Support (von wem und wo man technische Unterstützung erhalten kann).
- Bezeichnung, Nummer und Gültigkeitsdauer der Lizenz.

Um das Programm zu aktivieren, ist eine Internetverbindung erforderlich.

Um bei der Aktivierung eine Schlüsseldatei zu erhalten, ist ein Aktivierungscode erforderlich. Einen Aktivierungscode erhalten Sie beim Kauf des Programms. Für die Aktivierung von Kaspersky Internet Security bestehen folgende Möglichkeiten:

- **Kommerzielle Version aktivieren**. Wählen Sie diese Aktivierungsmethode, wenn Sie eine kommerzielle Programmversion erworben und Sie einen Aktivierungscode erhalten haben. Auf Basis dieses Codes bekommen Sie eine Schlüsseldatei, die Ihnen während der gesamten Laufzeit der Lizenz den Zugriff auf die volle Funktionsfähigkeit des Programms bietet.
- **Testversion aktivieren**. Wählen Sie diese Aktivierungsvariante, wenn Sie eine Testversion des Programms installieren möchten, bevor Sie über den Kauf einer kommerziellen Version entscheiden. Sie erhalten eine kostenlose Schlüsseldatei, deren Gültigkeitsdauer durch die Lizenz der Testversion dieses Programms beschränkt ist.

- **Später aktivieren**. Bei der Auswahl dieser Variante wird die Aktivierung von Kaspersky Internet Security übersprungen. Das Programm wird auf Ihrem Computer installiert und Sie können alle Programmfunktionen außer dem Update nutzen. (Kaspersky Internet Security kann nach der Installation nur einmal aktualisiert werden.) Die Variante **Später aktivieren** steht nur zur Verfügung, wenn der Aktivierungsassistent zum ersten Mal gleich nach der Programminstallation gestartet wird.

Wenn Kaspersky Internet Security früher installiert und dann gelöscht wurde, wobei die Informationen über die Aktivierung gespeichert wurden, dann fehlt dieser Schritt. In diesem Fall erhält der Konfigurationsassistent automatisch die Informationen über die vorhandene Lizenz, die im Fenster des Assistenten (s. S. 32) angezeigt werden.

SIEHE AUCH

Kommerzielle Version aktivieren 31

Testversion aktivieren..... 31

Aktivierung abschließen 32

KOMMERZIELLE VERSION AKTIVIEREN

Wenn diese Variante gewählt wird, erfolgt die Programmaktivierung über den Webserver von Kaspersky Lab. Dafür ist eine Internetverbindung erforderlich.

Die Aktivierung beruht auf der Eingabe des Aktivierungscodes, den Sie per E-Mail erhalten, wenn Sie Kaspersky Internet Security über das Internet kaufen. Wurde das Programm in einer CD-Box gekauft, dann ist der Aktivierungscode auf der Aktivierungskarte angegeben.

Der Aktivierungscode besteht aus einer durch Bindestriche getrennten Ziffernfolge mit vier Blöcken zu je fünf Ziffern ohne Leerzeichen. Zum Beispiel 11111-11111-11111-11111. Beachten Sie bitte, dass der Code in lateinischen Buchstaben eingegeben werden muss.

Der Aktivierungsassistent baut eine Verbindung mit dem Kaspersky-Lab-Aktivierungsserver im Internet auf und sendet Ihren Aktivierungscode an den Server, der den Code überprüft. Wenn der Aktivierungscode die Überprüfung besteht, erhält der Assistent eine Schlüsseldatei, die automatisch installiert wird. Der Aktivierungsvorgang wird abgeschlossen und auf dem Bildschirm erscheint ein Fenster mit ausführlichen Informationen über die erworbene Lizenz.

Wenn der Aktivierungscode die Überprüfung nicht bestanden hat, erscheint eine entsprechende Meldung auf dem Bildschirm. In diesem Fall sollten Sie sich an die Firma wenden, bei der Sie Kaspersky Internet Security gekauft haben.

Wenn die zulässige Anzahl der Aktivierungen für diesen Aktivierungscode überschritten wurde, erscheint eine entsprechende Meldung auf dem Bildschirm. Der Aktivierungsvorgang wird abgebrochen und das Programm schlägt Ihnen vor, sich an den Support von Kaspersky Lab zu wenden.

Wenn bei Verbindung mit dem Aktivierungsserver Fehler eingetreten sind und keine Schlüsseldatei heruntergeladen wurde, wenden Sie sich an den technischen Support.

TESTVERSION AKTIVIEREN

Wählen Sie diese Aktivierungsvariante, wenn Sie eine Testversion von Kaspersky Internet Security installieren möchten, bevor Sie über den Kauf einer kommerziellen Version entscheiden. Sie erhalten einen kostenlosen Schlüssel, dessen Gültigkeitsdauer durch den Lizenzvertrag der Testversion des Programms beschränkt ist. Nach Ablauf der Probelizenz ist es nicht möglich, eine weitere Probelizenz zu aktivieren.

Wenn bei Verbindung mit dem Aktivierungsserver Fehler eingetreten sind und keine Schlüsseldatei heruntergeladen wurde, wenden Sie sich an den technischen Support.

AKTIVIERUNG ABSCHLIEßEN

Der Aktivierungsassistent informiert Sie über den erfolgreichen Abschluss der Aktivierung von Kaspersky Internet Security. Außerdem werden Informationen über die Lizenz angezeigt: Typ (kommerziell, Test usw.), Gültigkeitsdauer der Lizenz, sowie Anzahl der Computer, für die die Lizenz gültig ist.

SCHRITT 2. SCHUTZMODUS AUSWÄHLEN

Wählen Sie einen Modus für den Schutz, der von Kaspersky Internet Security gewährleistet wird.

Es stehen zwei Modi zur Auswahl:

- *Automatisch*. Beim Eintreten wichtiger Ereignisse führt Kaspersky Internet Security automatisch die Aktion aus, die von den Kaspersky-Lab-Spezialisten empfohlen wird. Beim Fund einer Bedrohung versucht das Programm, das Objekt zu desinfizieren, und wenn die Desinfektion fehlschlägt, wird das Objekt gelöscht. Verdächtige Objekte werden unbearbeitet übersprungen. Über eingetretene Ereignisse wird durch Popupmeldungen informiert.

- *Interaktiv*. In diesem Modus reagiert das Programm so auf eintretende Ereignisse, wie Sie es festlegen. Beim Eintreten von Ereignissen, die Ihre Reaktion erfordern, zeigt das Programm eine Meldung (auf S. 207), in der eine Aktion gewählt werden kann.

Meldungen über den Fund einer aktiven Infektion werden unabhängig davon angezeigt, welcher Schutzmodus gewählt wurde.

SCHRITT 3. PROGRAMM-UPDATE ANPASSEN

Dieser Schritt des Konfigurationsassistenten wird übersprungen, wenn der Modus zur schnellen Installation gewählt wurde. Die Programmparameter, die bei diesem Schritt angepasst werden, erhalten Standardwerte.

Die Qualität des Schutzes Ihres Computers ist unmittelbar vom rechtzeitigen Download der Updates für die Datenbanken und Programm-Module abhängig. In diesem Fenster des Assistenten können Sie den Modus für das Update von Kaspersky Internet Security auswählen und Einstellungen für den Zeitplan vornehmen:

- **Automatisches Update**. Kaspersky Internet Security prüft in festgelegten Zeitabständen, ob an der Updatequelle ein Updatepaket vorhanden ist. Die Häufigkeit der Überprüfung kann während Viren-Epidemien steigen und unter gewöhnlichen Umständen sinken. Wenn neue Updates gefunden werden, lädt das Programm sie herunter und installiert sie auf dem Computer. Dieser Modus wird standardmäßig verwendet.

- **Update nach Zeitplan** (Das Intervall ist von den Zeitplaneinstellungen abhängig). Das Update wird automatisch nach einem festgelegten Zeitplan gestartet. Der Zeitplan wird in dem Fenster angepasst, das durch Klick auf die Schaltfläche **Einstellungen** geöffnet wird.

- **Manuelles Update**. In diesem Fall starten Sie das Programm-Update manuell.

Beachten Sie, dass die Datenbanken und Programm-Module, die in der Distribution enthalten sind, zum Zeitpunkt der Installation von Kaspersky Internet Security bereits veraltet sein können. Wir empfehlen deshalb, die aktuellen Updates für Kaspersky Internet Security herunterzuladen. Klicken Sie dazu auf die Schaltfläche **Jetzt aktualisieren**. In diesem Fall empfängt das Programm die erforderlichen Updates von den Updateseiten im Internet und installiert sie auf Ihrem Computer.

Wenn die im Lieferumfang enthaltenen Datenbanken stark veraltet sind, kann das Updatepaket relativ umfangreich sein und zusätzlichen Internet-Datenverkehr verursachen (bis zu mehrere Dutzend MB).

Wenn Sie die Updateparameter anpassen möchten (s. Abschnitt "Update" auf S. 151) (die Quelle wählen, von der das Update erfolgt; den Start des Updates mit den Rechten eines bestimmten Benutzerkontos anzupassen; den Dienst zum Kopieren von Updates in eine lokale Quelle aktivieren), klicken Sie auf die Schaltfläche **Einstellungen**.

SCHRITT 4. KONTROLLE DES ZUGRIFFS AUF DAS PROGRAMM

Dieser Schritt des Konfigurationsassistenten von Kaspersky Internet Security wird übersprungen, wenn der Modus zur schnellen Installation gewählt wurde. Die Programmparameter, die bei diesem Schritt angepasst werden, erhalten Standardwerte.

Da ein PC von mehreren Personen verwendet werden kann, die über ein unterschiedliches Maß an Fertigkeiten im Umgang mit Computern verfügen, und weil Schadprogramme versuchen können, den Schutz Ihres Computers auszuschalten, wird Ihnen angeboten, den Zugriff auf Kaspersky Internet Security mit Hilfe eines Kennworts zu beschränken. Das Kennwort erlaubt es, das Programm vor Versuchen zum unerlaubten Ausschalten des Schutzes oder zum Ändern der Einstellungen von Kaspersky Internet Security zu schützen.

Um den Kennwortschutz zu verwenden, aktivieren Sie das Kontrollkästchen ☑ **Kennwortschutz aktivieren** und füllen Sie die Felder **Neues Kennwort** und **Kennwort bestätigen** aus.

Geben Sie darunter den Bereich an, auf den sich die Zugriffsbeschränkung beziehen soll:

- ☑ **Programmparameter ändern** – Kennwortabfrage beim Versuch des Benutzers, geänderte Einstellungen von Kaspersky Internet Security zu speichern.
- ☑ **Programm beenden** – Kennwortabfrage beim Versuch des Benutzers, die Arbeit des Programms zu beenden.

SCHRITT 5. ERKENNBARE BEDROHUNGEN AUSWÄHLEN

Dieser Schritt des Konfigurationsassistenten wird übersprungen, wenn der Modus zur schnellen Installation gewählt wurde. Die Programmparameter, die bei diesem Schritt angepasst werden, erhalten Standardwerte.

Auf dieser Etappe können Sie die Kategorien der Bedrohungen auswählen, vor denen Kaspersky Internet Security Ihren Computer schützen soll. Programme, die Ihrem Computer Schaden zufügen können, werden immer von Kaspersky Internet Security überwacht. Dazu gehören die Programmtypen Viren, Würmer und trojanische Programme.

SCHRITT 6. ZWISCHENSPEICHERUNG VON DOMÄNENNAMEN (DNS) DEAKTIVIEREN

Dieser Schritt des Konfigurationsassistenten wird übersprungen, wenn der Modus zur schnellen Installation gewählt wurde. Die Programmparameter, die bei diesem Schritt angepasst werden, erhalten Standardwerte.

Der Dienst zur Zwischenspeicherung von Domänennamen verkürzt die Verbindungszeit Ihres Computers mit erforderlichen Internetressourcen wesentlich. Allerdings stellt er gleichzeitig eine gefährliche Schwachstelle dar, die von Angreifern benutzt werden kann, um Zugriff auf Ihre Daten zu erhalten.

Aktivieren Sie das Kontrollkästchen ☑ **DNS-Zwischenspeicherung deaktivieren**, um das Sicherheitsniveau für Ihren Computer zu erhöhen.

Das Deaktivieren der DNS-Zwischenspeicherung kann bei der Arbeit von Programmen, die eine Vielzahl von Netzwerkverbindungen benutzen (z.B. Clients für Dateiaustausch über Netzwerke), Probleme verursachen.

Bei diesem Schritt können Sie festlegen, ob im Schutzbericht Einträge über nicht kritische Ereignisse aufgezeichnet werden sollen. Aktivieren Sie dazu das Kontrollkästchen ☑ **Nicht kritische Ereignisse protokollieren**.

SCHRITT 7. SYSTEMANALYSE

Auf dieser Etappe werden Informationen über Programme, die zu Microsoft Windows gehören, gesammelt. Diese Programme werden in die Liste der vertrauenswürdigen Anwendungen aufgenommen, deren Aktionen im System nicht beschränkt werden.

SCHRITT 8. ASSISTENT ABSCHLIEßEN

Das letzte Fenster des Assistenten informiert über den Abschluss der Programminstallation. Um mit der Arbeit von Kaspersky Internet Security zu beginnen, vergewissern Sie sich, dass das Kontrollkästchen ☑ **Kaspersky Internet Security starten** aktiviert ist und klicken Sie auf die Schaltfläche **Beenden**.

NETZWERKTYP AUSWÄHLEN

Nach der Installation von Kaspersky Internet Security überwacht die Komponente Firewall die aktiven Netzwerkverbindungen auf Ihrem Computer. Jede Netzwerkverbindung erhält einen Status, der die erlaubte Netzwerkaktivität festlegt.

Wenn Sie für Kaspersky Internet Security den interaktiven Funktionsmodus ausgewählt haben (s. Abschnitt "Schritt 2. Schutzmodus auswählen" auf S. 32), wird beim Fund einer Netzwerkverbindung eine Meldung angezeigt. Im Meldungsfenster können Sie den Status des neuen Netzwerks festlegen:

- **Öffentliches Netzwerk**. Netzwerkverbindungen mit diesem Status wird der Zugriff auf Ihren Computer verboten. In einem solchen Netzwerk ist auch der Zugriff auf gemeinsame Ordner und Drucker untersagt. Es wird empfohlen, dem Internet diesen Status zuzuweisen.

- **Lokales Netzwerk**. Für Netzwerkverbindungen mit diesem Status wird der Zugriff auf gemeinsame Ordner und Netzwerkdrucker erlaubt. Es wird empfohlen, diesen Status für ein geschütztes lokales Netzwerk (z.B. Firmennetzwerk) zu verwenden.

- **Vertrauenswürdiges Netzwerk**. Netzwerkverbindungen mit diesem Status wird jede Aktivität erlaubt. Dieser Status wird nur für eine absolut sichere Zone empfohlen.

Für jeden Netzwerkstatus enthält der Lieferumfang von Kaspersky Internet Security eine Auswahl von Regeln zur Steuerung der Netzwerkaktivität. Der Status, den ein Netzwerk erhält, wenn es zum ersten Mal gefunden wird, kann später geändert werden.

PROGRAMM-UPDATE

Für das Update von Kaspersky Internet Security ist eine bestehende Internetverbindung erforderlich.

Zum Lieferumfang von Kaspersky Internet Security gehören Datenbanken mit Bedrohungssignaturen, Muster von typischen Spam-Phrasen und Beschreibungen von Netzwerkangriffen. Zum Zeitpunkt der Installation von Kaspersky Internet Security können die Datenbanken veraltet sein, weil die Datenbanken und Programm-Module regelmäßig von Kaspersky Lab aktualisiert werden.

Im Verlauf des Konfigurationsassistenten des Programms können Sie den Startmodus für Update (s. Abschnitt "Schritt 3. Programm-Update anpassen" auf S. 32) auswählen. Kaspersky Internet Security überprüft in der Grundeinstellung automatisch, ob auf den Kaspersky-Lab-Updateservern neue Updates vorhanden sind. Wenn auf dem Server neue Updates vorhanden sind, führt Kaspersky Internet Security im Hintergrundmodus den Download und die Installation der Updates durch.

Wenn die im Lieferumfang enthaltenen Datenbanken stark veraltet sind, kann das Updatepaket relativ umfangreich sein und zusätzlichen Internet-Datenverkehr verursachen (bis zu mehrere Dutzend MB).

Um den Schutz Ihres Computers aktuell zu halten, wird empfohlen, Kaspersky Internet Security sofort nach der Installation zu aktualisieren.

Gehen Sie folgendermaßen vor, um Kaspersky Internet Security auf Befehl zu aktualisieren:

1. Öffnen Sie das Programmhauptfenster.
2. Wählen Sie auf der linken Fensterseite den Abschnitt **Update** aus.
3. Klicken Sie auf die Schaltfläche **Update ausführen**.

VIRENUNTERSUCHUNG DES COMPUTERS

Die Autoren schädlicher Programme strengen sich sehr an, die Aktivität ihrer Programme zu verheimlichen. Deshalb kann es sein, dass Sie die Existenz von Malware auf Ihrem Computer nicht bemerken.

Bei der Installation von Kaspersky Internet Security wird automatisch die Aufgabe **Schnelle Untersuchung** ausgeführt. Diese Aufgabe dient der Suche und Neutralisierung von schädlichen Programmen in Objekten, die beim Hochfahren des Betriebssystems geladen werden.

Die Spezialisten von Kaspersky Lab empfehlen, zusätzlich die Aufgabe **Vollständige Untersuchung** auszuführen.

Gehen Sie folgendermaßen vor, um eine Untersuchungsaufgabe zu starten:

1. Öffnen Sie das Programmhauptfenster.
2. Wählen Sie auf der linken Fensterseite den Abschnitt **Untersuchung**.
3. Klicken Sie auf die Schaltfläche **Vollständige Untersuchung ausführen**, um die Untersuchung zu starten.

UNTERSUCHUNG DES COMPUTERS AUF SCHWACHSTELLEN

Aufgrund unerwünschter Aktivität auf Ihrem Computer, die durch Systemabstürze oder Aktivität schädlicher Programme verursacht werden kann, können den Einstellungen des Betriebssystems falsche Werte zugewiesen werden. Außerdem können auf Ihrem Computer installierte Programme Schwachstellen aufweisen, die Angreifern dazu dienen können, um Ihren Computer zu beschädigen.

Um derartige Sicherheitsprobleme zu erkennen und zu beheben, empfehlen die Kaspersky-Lab-Spezialisten, nach der Installation des Programms die *Aufgabe zur Suche nach Schwachstellen* (s. S. 147) zu starten. Im Verlauf der Aufgabenausführung wird in den installierten Programmen nach Schwachstellen und in den Einstellungen des Betriebssystems und des Browsers nach Beschädigungen und Anomalien gesucht.

Gehen Sie folgendermaßen vor, um die Aufgabe zur Schwachstellen-Suche zu starten:

1. Öffnen Sie das Programmhauptfenster.
2. Wählen Sie auf der linken Fensterseite den Abschnitt **Untersuchung**.
3. Klicken Sie auf die Schaltfläche **Fenster zur Suche nach Schwachstellen öffnen**.
4. Klicken Sie im folgenden Fenster auf die Schaltfläche **Suche nach Schwachstellen ausführen**.

LIZENZVERWALTUNG

Die Möglichkeit zur Benutzung von Kaspersky Internet Security wird durch das Vorhandensein einer Schlüsseldatei bestimmt. Eine Schlüsseldatei erhalten Sie mit Hilfe des Aktivierungscodes, der Ihnen beim Kauf des Programms zur Verfügung gestellt wird. Sie berechtigt Sie ab dem Tag der Aktivierung zur Nutzung des Programms. Der Schlüssel enthält Informationen zur Lizenz: Typ, Gültigkeitsdauer und Anzahl der Computer, für die die Lizenz gültig ist.

Wenn kein Schlüssel vorhanden ist und keine Testversion von Kaspersky Internet Security aktiviert wurde, wird das Programm in einem Modus funktionieren, in dem das Update nur ein einziges Mal möglich ist. Danach werden keine neuen Updates mehr ausgeführt.

Wenn eine Testversion des Programms aktiviert wurde, wird Kaspersky Internet Security nach dem Ablauf der Nutzungsdauer nicht mehr funktionieren.

Bei Ablauf der Gültigkeitsdauer einer kommerziellen Lizenz bleibt die Funktionalität des Programms unter Ausnahme der Updatemöglichkeit für die Programm-Datenbanken erhalten. Sie können Ihren Computer mit Hilfe der Untersuchungsaufgaben weiterhin untersuchen und die Schutzkomponenten verwenden, allerdings nur mit den Datenbanken, die bei Ablauf der Lizenz aktuell waren. Demzufolge können wir Ihnen keinen maximalen Schutz vor neuen Viren garantieren, die nach dem Gültigkeitsende der Lizenz gefunden werden.

Um eine Infektion Ihres Computers durch neue Viren zu verhindern, empfehlen wir Ihnen, die Lizenz für die Benutzung von Kaspersky Internet Security zu verlängern. Zwei Wochen vor Gültigkeitsende der Lizenz werden Sie vom Programm darüber benachrichtigt. Innerhalb eines bestimmten Zeitraums wird bei jedem Programmstart eine entsprechende Meldung auf dem Bildschirm angezeigt.

Informationen über die aktive Lizenz befinden sich im Fenster des **Lizenz-Managers**: Typ (kommerziell, Test), maximale Anzahl der Computer, auf denen diese Lizenz verwendet werden darf, Gültigkeitsdauer und Anzahl der bis zum Ablauf verbleibenden Tage.

Zu den Bedingungen des Lizenzvertrags über die Nutzung des Programms gelangen Sie über die Schaltfläche **Lizenzvertrag lesen**. Um eine Schlüsseldatei zu löschen, klicken Sie auf die Schaltfläche ✖, die sich rechts von der Lizenz befindet, deren Schlüsseldatei gelöscht werden soll. Um eine neue Lizenz zu aktivieren, verwenden Sie die Schaltfläche **Neue Lizenz aktivieren**.

Mit Hilfe der Schaltfläche **Lizenz kaufen (Lizenz verlängern**) können Sie zum Kauf (Verlängerung) einer Lizenz in den Online-Shop von Kaspersky Lab gehen.

Kaspersky Lab führt in regelmäßigen Zeitabständen Aktionen durch, bei denen Lizenzen für unsere Produkte zu besonders günstigen Preisen angeboten werden. Verfolgen Sie unsere Aktionen auf der Internetseite von Kaspersky Lab.

TEILNAHME AN KASPERSKY SECURITY NETWORK

Jeden Tag taucht eine Vielzahl neuer Bedrohungen auf. Um das Erstellen einer Statistik über neue Bedrohungstypen und ihre Quellen sowie die Entwicklung entsprechender Neutralisierungsmethoden zu beschleunigen, bietet Kaspersky Lab Ihnen die Teilnahme an dem Dienst Kaspersky Security Network an.

Bei der Verwendung von Kaspersky Security Network werden folgende Informationen an Kaspersky Lab gesendet:

- Unikaler Identifikator, den das Kaspersky Internet Security Ihrem Computer zugewiesen hat. Dieser Identifikator charakterisiert die Hardwareparameter Ihres Computers und enthält keinerlei persönliche Informationen.
- Informationen über die Bedrohungen, die von den Programmkomponenten gefunden wurden. Die Auswahl der Informationen ist vom Typ der gefundenen Bedrohung abhängig.
- Informationen über das System: Version des Betriebssystems, installierte Service Packs, geladene Dienste und Treiber, Versionen von Browsern und Mailprogrammen, Erweiterungen für Browser, Versionsnummer des installierten Kaspersky-Lab-Programms.

Im Rahmen von Kaspersky Security Network wird außerdem eine erweiterte Statistik erstellt. Dazu gehören Informationen über:

- auf Ihrem Computer geladene ausführbare Dateien und signierte Programme.
- auf Ihrem Computer gestartete Programme.

Die statistischen Informationen werden bei Abschluss des Programm-Updates gesendet.

Kaspersky Lab garantiert, dass im Rahmen von Kaspersky Security Network keine persönlichen Benutzerdaten gesammelt und gesendet werden.

➡ *Gehen Sie folgendermaßen vor, um Parameter für das Senden einer Statistik anzupassen:*

1. Öffnen Sie das Programmhauptfenster.
2. Wählen Sie auf der linken Fensterseite den Abschnitt **Feedback**.
3. Aktivieren Sie das Kontrollkästchen ☑ **Ich akzeptiere die Teilnahmebedingungen für Kaspersky Security Network**, um die Teilnahme an Kaspersky Security Network zu bestätigen.

SICHERHEITSVERWALTUNG

Auftretende Probleme beim Schutz des Computers signalisiert der Schutzstatus des Computers (s. Abschnitt "Hauptfenster von Kaspersky Internet Security" auf S. 43): Es ändert sich die Farbe des Schutzstatus-Symbols auch in der Leiste, wo es angezeigt wird. Wenn im Schutz Probleme auftreten, sollten diese umgehend behoben werden.

Abbildung 1: Aktueller Zustand des Computerschutzes

Durch Klick auf das Symbol für den Status oder auf die Leiste, auf der sich das Symbol befindet (s. Abbildung oben), gelangen Sie auf die Registerkarte **Status** (s. Abbildung unten), die eine Liste der aufgetretenen Probleme enthält und entsprechende Lösungsmöglichkeiten bietet.

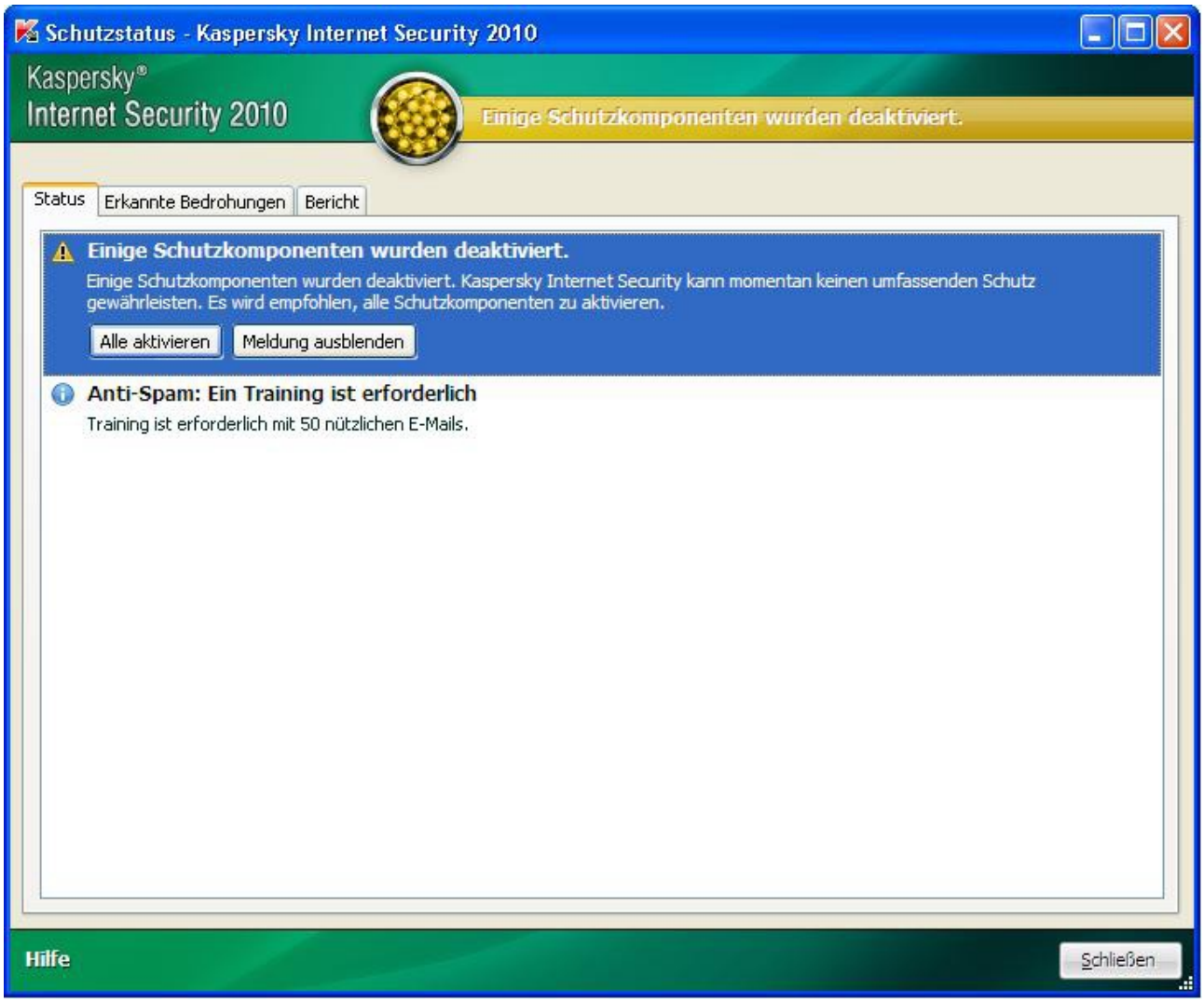
Schutzstatus - Kaspersky Internet Security 2010
Kaspersky®
Internet Security 2010
Einige Schutzkomponenten wurden deaktiviert.
Status
Erkannte Bedrohungen
Bericht
Einige Schutzkomponenten wurden deaktiviert.
Einige Schutzkomponenten wurden deaktiviert. Kaspersky Internet Security kann momentan keinen umfassenden Schutz gewährleisten. Es wird empfohlen, alle Schutzkomponenten zu aktivieren.
Alle aktivieren
Meldung ausblenden
Anti-Spam: Ein Training ist erforderlich
Training ist erforderlich mit 50 nützlichen E-Mails.
Hilfe
Schließen

Abbildung 2: Sicherheitsprobleme beheben

Sie können eine Liste der vorhandenen Probleme ansehen. Die Probleme sind ihrer Priorität entsprechend angeordnet und sollten in dieser Reihenfolge gelöst werden: Zu Beginn stehen die wichtigsten Probleme, die mit einem rotem Symbol gekennzeichnet sind, danach die weniger wichtigen mit gelbem Symbol und zum Schluss informative Meldungen. Für jedes Problem ist eine ausführliche Beschreibung vorhanden und folgende Aktionen werden angeboten:

- *Sofort beheben*. Mit Hilfe der entsprechenden Schaltflächen können Sie zur sofortigen Neutralisierung der Probleme übergehen, was der empfohlenen Aktion entspricht.

- *Behebung aufschieben*. Wenn das sofortige Beheben eines Problems aufgrund bestimmter Umstände nicht möglich ist, kann diese Aktion aufgeschoben werden und Sie können später dazu zurückkehren. Klicken Sie dazu auf die Schaltfläche **Meldung ausblenden**.

  Beachten Sie, dass diese Möglichkeit für kritische Probleme nicht vorgesehen ist. Dazu gehören beispielsweise die Existenz nicht neutralisierter schädlicher Objekte, Störungen bei der Arbeit einer oder mehrerer Komponenten, und beschädigte Programmdateien.

Um Meldungen, die zuvor ausgeblendet wurden, erneut in der Liste anzuzeigen, aktivieren Sie das Kontrollkästchen ☑ **Ausgeblendete Meldungen anzeigen**.

SIEHE AUCH:

Schutzstatus 39

SCHUTZSTATUS

Die Arbeit der Komponenten von Kaspersky Internet Security oder der Untersuchungsaufgaben wird im Abschnitt Statistik dokumentiert, der Informationen über den Zustand des Computerschutzes enthält. Hier können Sie erfahren, wie viele gefährliche und verdächtige Objekte das Programm gefunden hat und welche dieser Objekte desinfiziert, gelöscht oder in die Quarantäne verschoben worden sind.

Wenn das Programm schädliche Objekte gefunden hat, wird dies durch den Schutzstatus des Computers signalisiert (s. Abschnitt "Hauptfenster von Kaspersky Internet Security" auf S. 43), indem sich die Farbe des Schutzstatussymbols und der Leiste, auf der sich das Symbol befindet, verändert. Beim Fund schädlicher Objekte ändert sich die Farbe des Symbols und der Leiste in Rot. In diesem sollten alle vorhandenen Bedrohungen umgehend neutralisiert werden.

- *Gehen Sie folgendermaßen vor, um sich über den Zustand des Computerschutzes zu informieren:*

  1. Öffnen Sie das Programmhauptfenster.
  2. Klicken Sie auf den Link **Bericht**.

- *Gehen Sie folgendermaßen vor, um im Computerschutz vorhandene Probleme zu beheben:*

  1. Öffnen Sie das Programmhauptfenster.
  2. Klicken Sie auf den Link **Bericht**.
  3. Führen Sie im folgenden Fenster auf der Registerkarte **Status** die entsprechenden Aktionen aus. Um Meldungen, die zuvor ausgeblendet wurden, erneut in der Liste anzuzeigen, aktivieren Sie das Kontrollkästchen **Ausgeblendete Meldungen anzeigen**.

- *Gehen Sie folgendermaßen vor, um eine Aktion mit einem gefundenen Objekt auszuführen:*

  1. Öffnen Sie das Programmhauptfenster.
  2. Klicken Sie auf den Link **Bericht**.
  3. Wählen Sie im folgenden Fenster auf der Registerkarte **Erkannte Bedrohungen** in der Liste das entsprechende Objekt aus und klicken Sie mit der rechten Maustaste darauf.
  4. Wählen Sie im Kontextmenü die erforderliche Aktion aus.

- *Gehen Sie folgendermaßen vor, um einen Bericht über die Arbeit der Schutzkomponenten zu lesen:*

  1. Öffnen Sie das Programmhauptfenster.
  2. Klicken Sie auf den Link **Bericht**.
  3. Wählen Sie im folgenden Fenster die Registerkarte **Bericht** aus.

SIEHE AUCH:

Sicherheitsverwaltung 37

SCHUTZ ANHALTEN

Das Anhalten des Schutzes bedeutet, dass alle Komponenten für einen bestimmten Zeitraum ausgeschaltet werden.

Durch das vorübergehende Deaktivieren wird die Arbeit aller Schutzkomponenten angehalten. Darüber informieren:

- Das inaktive (graue) Programmsymbol (s. Abschnitt "Symbol im Infobereich der Taskleiste" auf S. 41) im Infobereich der Taskleiste;
- Rote Farbe von Statussymbol und Leiste im Hauptfenster von Kaspersky Internet Security.

Wenn im Augenblick, als der Schutz beendet wurde, auf dem Computer Netzwerkverbindungen aktiv waren, erscheint auf dem Bildschirm eine Meldung darüber, dass diese Verbindungen getrennt werden.

Gehen Sie folgendermaßen vor, um den Computerschutz anzuhalten:

1. Im Kontextmenü (s. Abschnitt "Kontextmenü" auf S. 42) des Programms wählen Sie den Punkt **Schutz anhalten**.
2. Wählen Sie im folgenden Fenster **Schutz anhalten** den Zeitraum, nach dem der Schutz wieder aktiviert werden soll:
   - **Anhalten für <Zeitintervall> -** Der Schutz wird nach Ablauf des festgelegten Zeitraums wieder aktiviert Wählen Sie in der Dropdown-Liste einen Wert für den Zeitraum aus.
   - **Anhalten bis zum Neustart –** Der Schutz wird nach dem Neustart des Programms oder des Systems aktiviert (unter der Bedingung, dass die Funktion zum Start von Kaspersky Internet Security beim Hochfahren des Systems aktiviert ist).
   - **Anhalten –** Der Schutz wird erst dann wieder aktiviert, wenn Sie ihn starten. Wählen Sie den Punkt **Schutz fortsetzen** im Kontextmenü des Programms, um den Schutz zu aktivieren.

PROGRAMMOBERFLÄCHE

Kaspersky Internet Security bietet eine intuitive bedienbare und komfortable Oberfläche. In diesem Kapitel werden die wichtigsten Elemente der Oberfläche ausführlich beschrieben.

Kaspersky Internet Security verfügt über Erweiterungskomponenten (Plug-ins), die in folgende Programme integriert werden können: Microsoft Office Outlook (Virensuche und Spam-Untersuchung), Microsoft Outlook Express (Spam-Untersuchung), The Bat! (Virensuche und Spam-Untersuchung), Thunderbird (Spam-Untersuchung), Microsoft Internet Explorer, Microsoft Windows Explorer. Die Plug-ins erweitern die Möglichkeiten der genannten Programme, weil die Steuerung und Konfiguration der Komponenten **Mail-Anti-Virus** und **Anti-Spam** direkt aus ihrer Programmoberfläche möglich ist.

IN DIESEM ABSCHNITT

Symbol im Infobereich der Taskleiste 41

Kontextmenü 42

Hauptfenster von Kaspersky Internet Security 43

Meldungen 46

Programmkonfigurationsfenster 46

SYMBOL IM INFOBEREICH DER TASKLEISTE

Sofort nach der Installation von Kaspersky Internet Security erscheint sein Symbol im Infobereich der Taskleiste von Microsoft Windows.

Das Symbol dient als Indikator für die Arbeit des Programms. Es informiert über den Schutzstatus und zeigt eine Reihe wichtiger Aktionen, die vom Programm ausgeführt werden.

Wenn das Symbol aktiv (farbig) ist, bedeutet es, dass der Schutz vollständig aktiviert ist oder bestimmte Schutzkomponenten aktiv sind. Wenn das Symbol inaktiv (schwarzweiß) ist, dann wurden alle Schutzkomponenten deaktiviert.

Abhängig von der momentan ausgeführten Operation verändert sich das Symbol von Kaspersky Internet Security:

- – Die Untersuchung einer E-Mail-Nachricht wird ausgeführt.
- – Das Update der Datenbanken und der Programm-Module wird ausgeführt.
- – Der Neustart des Computers ist erforderlich, um die Updates zu übernehmen.
- – Bei der Arbeit einer Programmkomponente ist eine Störung aufgetreten.

Außerdem sorgt das Symbol für den Zugang zu den Grundelementen der Programmoberfläche: Kontextmenü (s. Abschnitt "Kontextmenü" auf S. 42) und Hauptfenster (s. Abschnitt "Hauptfenster von Kaspersky Internet Security" auf S. 43).

Das Kontextmenü wird durch Rechtsklick auf das Programmsymbol geöffnet.

Um das Hauptfenster von Kaspersky Internet Security zu öffnen, klicken Sie mit der linken Maustaste auf das Programmsymbol.

Wenn Neuigkeiten von Kaspersky Lab erschienen sind, wird im Infobereich der Taskleiste von Microsoft Windows das Symbol eingeblendet. Der Nachrichtentext wird durch Doppelklick auf das entsprechende Symbol geöffnet.

KONTEXTMENÜ

Das Kontextmenü bietet Zugriff auf die wichtigsten Schutzaufgaben.

Das Menü von Kaspersky Internet Security enthält folgende Punkte:

- **Update** - Starten der Aktualisierung der Datenbanken und Module des Programms und der Installation der Updates auf Ihrem Computer.
- **Computer vollständig untersuchen** – Starten der vollständigen Untersuchung Ihres Computers auf das Vorhandensein schädlicher Objekte. Dabei werden die Objekte auf allen Laufwerken einschließlich der Wechseldatenträger untersucht.
- **Auf Viren untersuchen** - Zur Auswahl von Objekten und zum Start der Virensuche wechseln. In der Grundeinstellung enthält die Liste eine Reihe von Objekten wie beispielsweise den Ordner **Eigene Dateien** und Mailboxen. Sie können die Liste ergänzen, Untersuchungsobjekte auswählen und die Virensuche starten.
- **Netzwerkmonitor** – Liste der bestehenden Netzwerkverbindungen (s. Abschnitt "Netzwerkmonitor" auf S. 198), der offenen Ports und des Datenverkehrs anzeigen.
- **Virtuelle Tastatur** - zu der virtuellen Tastatur wechseln.
- **Kaspersky Internet Security** – Programmhauptfenster öffnen (s. Abschnitt "Programmhauptfenster von Kaspersky Internet Security" auf S. 43).
- **Einstellungen** – Zur Anzeige und Konfiguration der Funktionsparameter des Programms wechseln.
- **Aktivierung** – zur Aktivierung von Kaspersky Internet Security gehen. Um den Status eines registrierten Benutzers zu erhalten, muss Ihre Version des Programms aktiviert werden. Dieser Menüpunkt ist nur vorhanden, wenn das Programm noch nicht aktiviert wurde.
- **Über das Programm** – Informationsfenster aufrufen, in dem Programminformationen angezeigt werden.
- **Schutz anhalten / Schutz fortsetzen** – zeitweises Ausschalten / Einschalten von Komponenten des Echtzeitschutzes. Dieser Menüpunkt bezieht sich nicht auf das Programm-Update und die Ausführung von Aufgaben zur Virensuche.
- **Netzwerk-Datenverkehr blockieren / Netzwerk-Datenverkehr freigeben** – vorübergehende Sperrung / Entsperrung aller Verbindungen des Computers.
- **Kindersicherung** – schnelles Umschalten zwischen aktiven Profilen der Komponente (s. Abschnitt "Kindersicherung" auf S. 126). Dieser Menüpunkt ist nur vorhanden, wenn die Kindersicherung gestartet und die Arbeit mit Profilen eingestellt wurde.

- **Beenden** – Arbeit von Kaspersky Internet Security beenden (bei Auswahl dieses Menüpunkts wird das Programm aus dem Arbeitsspeicher des Computers entfernt).

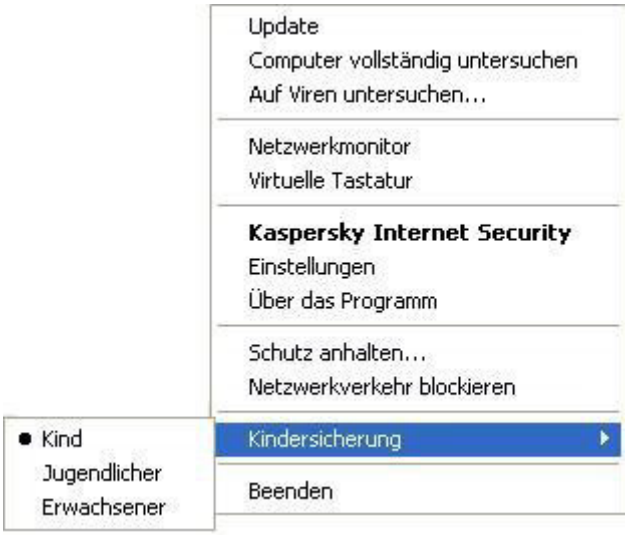

Abbildung 3: Kontextmenü

Wird das Kontextmenü geöffnet, während eine Aufgabe zur Virensuche läuft, so wird ihr Name mit Prozentangabe des Ausführungsergebnisses im Kontextmenü angezeigt. Durch die Auswahl der Aufgabe gelangen Sie in das Hauptfenster mit dem Bericht über ihre aktuellen Ausführungsergebnisse.

HAUPTFENSTER VON KASPERSKY INTERNET SECURITY

Das Programmhauptfenster lässt sich bedingt in drei Bereiche aufteilen:

- Der obere Bereich des Fensters informiert über den aktuellen Schutzstatus Ihres Computers.

Abbildung 4: Aktueller Zustand des Computerschutzes

Es gibt drei Varianten für den Schutzstatus. Jeder Status wird durch eine bestimmte Farbe signalisiert. Die Farben entsprechen den Signalen einer Ampel. Die Farbe Grün bedeutet, dass der Schutz Ihres Computers dem erforderlichen Niveau entspricht. Gelb und Rot signalisieren, dass bestimmte Sicherheitsbedrohungen vorliegen. Als Bedrohung gilt nicht nur der Fund schädlicher Programme, sondern auch die Verwendung veralteter Datenbanken, die deaktivierten Schutzkomponenten, die Auswahl einer niedrigen Sicherheitsstufe u.a.

Vorhandene Sicherheitsrisiken sollten umgehend behoben werden. Um ausführliche Informationen darüber zu erhalten und die Bedrohungen schnell zu beheben, verwenden Sie den Assistenten zu Sicherheitsverwaltung oder klicken Sie auf das Symbol für den Status oder für die Leiste, auf der sich das Symbol befindet (s. Abbildung oben).

- Die linke Seite des Fensters bietet schnellen Zugriff auf alle Programmfunktionen, auf die Ausführung von Aufgaben zur Virensuche oder zum Update, u.a.

Abbildung 5: Linker Teil des Hauptfensters

- Die rechte Seite des Fensters enthält Informationen über die auf der linken Seite ausgewählte Programmfunktion und erlaubt es, Parameter anzupassen, bietet Werkzeuge zum Ausführen von Aufgaben zur Virensuche, zum Update-Download, u.a.

Schutz-Center für Ihren Computer
Kaspersky Internet Security schützt die Daten auf dem Computer vor Schadprogrammen und unerlaubtem Zugriff, und gewährleistet den sicheren Zugriff auf das lokale Netzwerk und auf das Internet
Dateien und persönliche Daten
Dokumente und Media-Dateien. Zugriffsparameter auf die unterschiedliche Ressourcen (Benutzernamen und Kennwörter), Daten für Kreditkarten u.a.
System und Programme
Auf Ihrem Computer installierte Programme und Objekte des Betriebssystems
Arbeit im Netzwerk
Anzeige von Webseiten, Verwendung von Zahlungssystemen. E-Mail (Schutz vor Spam und Viren). Instant Messenger (ICQ, MSN u.a.)
Netzwerkmonitor
Insgesamt untersuchte Objekte: 882
Erkannte Bedrohungen: 0
Virus: 0
Trojanisches Programm: 0
Schädliches Tool: 0
Adware: 0
Unerwünschte Software: 0

Abbildung 6: Rechter Teil des Hauptfensters

Außerdem stehen folgende Schaltflächen und Links zur Verfügung:

- **Einstellungen** – in das Programmkonfigurationsfenster wechseln.
- **Quarantäne** – zur Arbeit mit Objekten, die in die Quarantäne verschoben wurden, wechseln.
- **Bericht** – zu einer Liste der Ereignisse, die bei der Arbeit des Programms eingetreten sind, wechseln.
- **Hilfe** – zum Hilfesystem für Kaspersky Internet Security wechseln.
- **Mein Kaspersky Account** – in den persönlichen Bereich des Benutzers (https://my.kaspersky.de) auf der Seite des technischen Supports gehen.
- **Support** - Das Fenster mit Informationen über das System und mit Links zu Informationsressourcen von Kaspersky Lab (Webseite des technischen Supports, Forum) öffnen.
- **Lizenz** – zur Aktivierung von Kaspersky Internet Security bzw. zur Verlängerung der Lizenz wechseln.

Sie können das Aussehen von Kaspersky Internet Security verändern, indem Sie grafische Elemente und Farbschemen erstellen und verwenden.

MELDUNGEN

Wenn bei der Arbeit von Kaspersky Internet Security bestimmte Ereignisse eintreten, werden Sie durch Popupmeldungen über dem Programmsymbol im Infobereich der Taskleiste von Microsoft Windows darüber informiert.

In Abhängigkeit davon, welche Relevanz das Ereignis für die Computersicherheit besitzt, sind folgende Arten von Meldungen möglich:

- **Alarm**. Ein Ereignis mit kritischer Priorität ist eingetreten. Beispiele: Ein Virus wurde gefunden oder im System wurde gefährliche Aktivität erkannt. Die sofortige Entscheidung über das weitere Vorgehen ist erforderlich. Meldungen dieses Typs sind rot gekennzeichnet.

- **Warnung**. Ein potentiell gefährliches Ereignis hat sich ereignet. Beispiele: "Ein möglicherweise infiziertes Objekt wurde gefunden" oder "Im System wurde verdächtige Aktivität erkannt". Sie werden aufgefordert, über die Gefährlichkeit dieses Ereignisses zu entscheiden. Meldungen dieses Typs sind gelb gekennzeichnet.

- **Info**. Diese Meldung informiert über ein Ereignis, das keine vorrangige Priorität besitzt. Zu diesem Typ zählen beispielsweise Meldungen, die bei der Arbeit der Komponente Inhaltsfilterung vorkommen. Informative Meldungen dieses Typs sind grün gekennzeichnet.

SIEHE AUCH

Meldungen.....207

PROGRAMMKONFIGURATIONSFENSTER

Das Konfigurationsfenster für die Einstellung von Kaspersky Internet Security lässt sich aus dem Hauptfenster (s. Abschnitt "Hauptfenster von Kaspersky Internet Security" auf S. 43) oder aus dem Kontextmenü (s. Abschnitt "Kontextmenü" auf S. 42) öffnen. Klicken Sie dazu im oberen Bereich des Hauptfensters auf den Link **Einstellungen** oder wählen Sie den gleichnamigen Punkt im Kontextmenü des Programms aus.

Das Konfigurationsfenster besteht aus zwei Teilen:

- Die linke Seite des Fensters bietet Zugriff auf die Funktionen von Kaspersky Internet Security, auf Untersuchungs- und Updateaufgaben usw.

- Die rechte Seite des Fensters enthält eine Liste von Parametern für die auf der linken Seite ausgewählte Komponente, Aufgabe usw.

SIEHE AUCH

Programmparameter anpassen.....157

SCHUTZ FÜR DAS DATEISYSTEM DES COMPUTERS

Datei-Anti-Virus erlaubt es, das Dateisystem des Computers vor einer Infektion zu schützen. Die Komponente wird beim Hochfahren des Betriebssystems gestartet, befindet sich ständig im Arbeitsspeicher des Computers und untersucht alle Dateien, die geöffnet, gespeichert und gestartet werden.

In der Grundeinstellung untersucht Datei-Anti-Virus nur neue oder veränderte Dateien. Die Untersuchung von Dateien erfolgt mit einer bestimmten Auswahl von Parametern, die als Sicherheitsstufe bezeichnet wird. Beim Fund von Bedrohungen führt Datei-Anti-Virus die festgelegte Aktion aus.

Das Schutzniveau für die Dateien und den Speicher auf Ihrem Computer wird durch folgende Gruppen von Parametern definiert:

- Parameter, die den Schutzbereich festlegen.
- Parameter, die die verwendete Untersuchungsmethode festlegen.
- Parameter, die die Untersuchung von zusammengesetzten Dateien (einschließlich der Untersuchung umfangreicher zusammengesetzter Dateien) festlegen.
- Parameter, die den Untersuchungsmodus festlegen.
- Parameter, die es erlauben, die Arbeit der Komponente nach Zeitplan oder während der Arbeit bestimmter Programme anzuhalten.

Die Spezialisten von Kaspersky Lab warnen davor, die Funktionsparameter von Datei-Anti-Virus zu verändern. In den meisten Fällen ist es ausreichend, die Sicherheitsstufe zu ändern. Sie können die Standardeinstellungen von Datei-Anti-Virus wiederherstellen. Wählen Sie dazu eine Sicherheitsstufe aus.

➡ *Gehen Sie folgendermaßen vor, um die Funktionsparameter von Datei-Anti-Virus anzupassen:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Datei-Anti-Virus** aus.
3. Klicken Sie für die ausgewählte Komponente auf die Schaltfläche **Einstellungen**.
4. Passen Sie die Parameter der Komponente entsprechend an.

IN DIESEM ABSCHNITT

Algorithmus für die Arbeit der Komponente 48

Sicherheitsstufe für Dateien und Speicher ändern 49

Aktion für gefundene Objekte ändern 49

Schutzbereich festlegen 50

Heuristische Analyse verwenden 51

Untersuchung optimieren 52

Untersuchung von zusammengesetzten Dateien 52

Untersuchung umfangreicher zusammengesetzter Dateien 52

Untersuchungsmodus ändern 53

Untersuchungstechnologie 53

Komponente anhalten: Zeitplan erstellen 54

Komponente anhalten: Liste der Programme erstellen 55

Standardmäßige Schutzparameter wiederherstellen 56

ALGORITHMUS FÜR DIE ARBEIT DER KOMPONENTE

Datei-Anti-Virus wird beim Hochfahren des Betriebssystems gestartet, befindet sich ständig im Arbeitsspeicher des Computers und untersucht alle Dateien, die geöffnet, gespeichert und gestartet werden.

Standardmäßig untersucht Datei-Anti-Virus nur neue oder veränderte Dateien, d.h. Dateien, die seit dem letzten Zugriff hinzugefügt oder verändert wurden. Die Untersuchung einer Datei erfolgt nach folgendem Algorithmus:

1. Die Komponente fängt den Zugriff des Benutzers oder eines bestimmten Programms auf eine beliebige Datei ab.

2. Datei-Anti-Virus prüft, ob in den Datenbanken iChecker und iSwift Informationen über die abgefangene Datei vorhanden sind. Auf Basis dieser Informationen wird entschieden, ob eine Untersuchung der Datei erforderlich ist.

Bei der Untersuchung werden folgende Aktionen ausgeführt:

1. Die Datei wird auf das Vorhandensein von Viren untersucht. Das Erkennen von Objekten erfolgt auf Basis der Datenbanken von Kaspersky Internet Security. Die Datenbanken enthalten eine Beschreibung aller momentan bekannten Schadprogramme, Bedrohungen, Netzwerkangriffe und entsprechende Desinfektionsmethoden.

2. Aufgrund der Analyseergebnisse sind folgende Varianten für das Verhalten von Kaspersky Internet Security möglich:

   a. Wenn in der Datei schädlicher Code gefunden wird, sperrt der Datei-Anti-Virus die Datei, erstellt seine Sicherungskopie und versucht, die Desinfektion durchzuführen. Bei erfolgreicher Desinfektion wird die Datei zum Zugriff freigegeben. Wenn die Desinfektion fehlschlägt, wird die Datei gelöscht.

   b. Wenn in der Datei ein Code gefunden wird, der Ähnlichkeit mit schädlichem Code besitzt, jedoch keine hundertprozentige Sicherheit darüber besteht, wird die Datei der Desinfektion unterzogen und in den Quarantänespeicher verschoben.

c. Wenn in der Datei kein schädlicher Code gefunden wird, wird sie sofort zum Zugriff freigegeben.

Beim Fund eines infizierten oder möglicherweise infizierten Objekts werden Sie vom Programm darüber informiert. Beim Fund eines infizierten oder möglicherweise infizierten Objekts erscheint auf dem Bildschirm eine Meldung mit einer Anfrage für das weitere Vorgehen. Ihnen wird vorgeschlagen:

- Der Start des Objekts wird auf dem Computer gesperrt oder der Benutzer wird nach den weiteren Aktionen gefragt: Die Bedrohung in die Quarantäne verschieben, um sie später mit Hilfe aktualisierter Datenbanken zu untersuchen und zu bearbeiten.
- Das Objekt löschen.
- Objekt überspringen, wenn Sie absolut sicher sind, dass es unschädlich ist.

SICHERHEITSSTUFE FÜR DATEIEN UND SPEICHER ÄNDERN

Unter Sicherheitsstufe wird eine vordefinierte Auswahl von Parametern für Datei-Anti-Virus verstanden. Die Spezialisten von Kaspersky Lab haben drei Sicherheitsstufen vordefiniert. Sie treffen selbst eine Entscheidung über die Auswahl der Sicherheitsstufe, wobei die Arbeitsbedingungen und die aktuelle Situation berücksichtigt werden sollten. Für die Sicherheitsstufe stehen folgende Varianten zur Auswahl:

- **Hoch**. Wählen Sie diese Stufe, wenn Sie das Infektionsrisiko für Ihren Computer sehr hoch einschätzen.
- **Empfohlen**. Diese Stufe bietet ein ausgewogenes Verhältnis zwischen Leistung und Sicherheit. Sie ist für die meisten Situationen geeignet.
- **Niedrig**. Wenn Sie in einer geschützten Umgebung arbeiten (z.B. in einem Firmennetzwerk mit zentralem Sicherheitssystem), ist die niedrige Sicherheitsstufe geeignet. Die niedrige Sicherheitsstufe kann auch bei der Arbeit mit ressourcenaufwändigen Programmen gewählt werden.

Es wird empfohlen, vor der Auswahl der niedrigen Sicherheitsstufe die vollständige Untersuchung des Computers mit der hohen Sicherheitsstufe vorzunehmen.

Wenn keine vordefinierte Stufe Ihren Anforderungen entspricht, können Sie die Einstellungen (s. Abschnitt "Schutz des Computer-Dateisystems" auf S. 47) von Datei-Anti-Virus anpassen. Dadurch ändert sich der Name der Sicherheitsstufe in **Benutzerdefiniert**. Um die standardmäßigen Einstellungen der Komponente wiederherzustellen, wählen Sie eine der vordefinierten Stufen aus.

➡ *Gehen Sie folgendermaßen vor, um die festgelegte Sicherheitsstufe für Dateien und Speicher zu ändern:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Datei-Anti-Virus** aus.
3. Legen Sie die erforderliche Sicherheitsstufe für die gewählte Komponente fest.

AKTION FÜR GEFUNDENE OBJEKTE ÄNDERN

Datei-Anti-Virus weist gefundenen Objekten aufgrund der Untersuchungsergebnisse einen der folgenden Status zu:

- Status eines der schädlichen Programme (beispielsweise *Virus*, *trojanisches Programm*).
- Status *möglicherweise infiziert*, wenn sich aufgrund der Untersuchung nicht eindeutig feststellen lässt, ob das Objekt infiziert ist oder nicht. Das bedeutet, dass in der Datei die Codefolge eines unbekannten Virus oder der modifizierte Code eines bekannten Virus gefunden wurde.

Wenn Kaspersky Internet Security bei einer Untersuchung infizierte oder möglicherweise infizierte Objekte findet, werden Sie darüber informiert. Sie werden dazu aufgefordert, auf die gefundene Bedrohung zu reagieren, indem Sie eine Aktion für das Objekt auswählen. Standardmäßig ist in Kaspersky Internet Security als Aktion für ein gefundenes Objekt die Variante **Aktion erfragen** festgelegt. Sie können die Aktion ändern. Wenn Sie beispielsweise sicher sind, dass versucht werden soll, alle gefundenen Objekte zu desinfizieren, und bei einer Meldung über den Fund eines infizierten oder verdächtigen Objekts nicht jedes Mal die Aktion **Desinfizieren** auswählen möchten, dann legen Sie folgende Aktion fest: **Aktion ausführen. Desinfizieren**.

Bevor ein infiziertes Objekt desinfiziert oder gelöscht wird, legt Kaspersky Internet Security eine Sicherungskopie des Objekts an. Dadurch wird erlaubt, das Objekt bei Bedarf wiederherzustellen oder später zu desinfizieren.

Wenn Sie im automatischen Modus (s. Abschnitt "Schritt 2. Schutzmodus auswählen" auf S. 32) arbeiten, wendet Kaspersky Internet Security automatisch die von den Kaspersky-Lab-Fachleuten empfohlene Aktion an, wenn gefährliche Objekte erkannt werden. Für schädliche Objekte ist dies die Aktion **Desinfizieren. Löschen, wenn Desinfektion nicht möglich**, für verdächtige Objekte ist es **Überspringen**.

Gehen Sie folgendermaßen vor, um die festgelegte Aktion für gefundene Objekte zu ändern:

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Datei-Anti-Virus** aus.
3. Geben Sie die entsprechende Aktion für die gewählte Komponente an.

SCHUTZBEREICH FESTLEGEN

Unter dem Schutzbereich wird nicht nur der Ort der Untersuchungsobjekte verstanden, sondern auch der Typ der zu untersuchenden Dateien. Kaspersky Internet Security untersucht standardmäßig nur potentiell infizierbare Dateien, die von beliebigen Festplatten, Wechseldatenträgern und Netzlaufwerken aus gestartet werden.

Sie können den Schutzbereich erweitern oder einschränken, indem Sie Untersuchungsobjekte hinzufügen / entfernen oder die Typen der zu untersuchenden Dateien ändern. Sie können beispielsweise nur *exe*-Dateien, die von Netzlaufwerken aus gestartet werden, untersuchen lassen. Allerdings sollten Sie sicherstellen, dass eine Einschränkung des Schutzbereichs nicht zu einem Sicherheitsrisiko für Ihren Computer führt.

Bei der Auswahl des Dateityps muss Folgendes beachtet werden:

- Es gibt eine Reihe von Dateiformaten (z.B. *txt*), für die das Risiko des Eindringens von schädlichem Code und dessen späterer Aktivierung relativ gering ist. Gleichzeitig gibt es Formate, die ausführbaren Code enthalten oder enthalten können (*exe*, *dll*, *doc*). Das Risiko, dass schädlicher Code in solche Dateien eindringt und später aktiviert wird, ist relativ hoch.
- Ein Angreifer kann einen Virus in einer Datei mit der Erweiterung *txt* an Ihren Computer senden, obwohl es sich dabei in Wirklichkeit um eine ausführbare Datei handelt, die in eine *txt*-Datei umbenannt wurde. Wenn die Variante **Dateien nach Erweiterung untersuchen** gewählt wurde, wird eine solche Datei bei der Untersuchung übersprungen. Wurde die Variante **Dateien nach Format untersuchen** gewählt, so ignoriert Datei-Anti-Virus die Erweiterung und analysiert die Kopfzeile der Datei, wodurch sich ergeben kann, dass die Datei das Format *exe* besitzt. Eine solche Datei wird der sorgfältigen Virusuntersuchung unterzogen.

Gehen Sie folgendermaßen vor, um die Liste der Untersuchungsobjekte zu ändern:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Datei-Anti-Virus** aus.
3. Klicken Sie für die ausgewählte Komponente auf die Schaltfläche **Einstellungen**.

4. Klicken Sie auf der Registerkarte **Allgemein** im Abschnitt **Schutzbereich** auf den Link **Hinzufügen**.

5. Wählen Sie im Fenster **Untersuchungsobjekt auswählen** ein Objekt aus und klicken Sie auf **Hinzufügen**.

6. Nachdem alle erforderlichen Objekte hinzugefügt wurden, klicken Sie im Fenster **Untersuchungsobjekt auswählen** auf die Schaltfläche **OK**.

7. Um bestimmte Objekte aus der Untersuchungsliste auszuschließen, deaktivieren Sie das entsprechende Kontrollkästchen.

Gehen Sie folgendermaßen vor, um den Typ der zu untersuchenden Dateien zu ändern:

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.

2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Datei-Anti-Virus** aus.

3. Klicken Sie für die ausgewählte Komponente auf die Schaltfläche **Einstellungen**.

4. Wählen Sie auf der Registerkarte **Allgemein** im Abschnitt **Dateitypen** den gewünschten Parameter.

HEURISTISCHE ANALYSE VERWENDEN

In der Grundeinstellung erfolgt die Untersuchung auf Basis der Datenbanken, die eine Beschreibung der bekannten Bedrohungen und entsprechende Desinfektionsmethoden enthalten. Kaspersky Internet Security vergleicht ein gefundenes Objekt mit den Einträgen in den Datenbanken, wodurch sich eindeutig ermitteln lässt, ob das untersuchte Objekt schädlich ist und welcher Malware-Klasse es gegebenenfalls angehört. Dieses Vorgehen wird als *Signaturanalyse* bezeichnet und wird standardmäßig verwendet.

Allerdings tauchen jeden Tag neue schädliche Objekte auf, die noch nicht in die Datenbanken aufgenommen wurden. Bei der Erkennung solcher Objekte hilft die heuristische Analyse. Diese Methode umfasst die Analyse der Aktivität, die ein Objekt im System zeigt. Wenn diese Aktivität als typisch für schädliche Objekte gilt, lässt sich ein Objekt mit hoher Wahrscheinlichkeit als schädlich oder verdächtig einstufen. Dadurch können neue Bedrohungen bereits erkannt werden, bevor die Virenanalytiker von ihrer Aktivität wissen.

Beim Fund eines schädlichen Objekts erhalten Sie eine Meldung mit einer Anfrage für das weitere Vorgehen.

Zusätzlich kann das Genauigkeitsniveau der Untersuchung festlegt werden. Es reguliert das Verhältnis zwischen Ausführlichkeit der Suche, Auslastungsniveau der Betriebssystemressourcen und Untersuchungsdauer. Je höher das für die Untersuchung gewählte Niveau, desto mehr Systemressourcen sind dafür erforderlich und desto mehr Zeit wird beansprucht.

Gehen Sie folgendermaßen vor, um die heuristische Analyse zu verwenden und die Untersuchungsgenauigkeit festzulegen:

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.

2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Datei-Anti-Virus** aus.

3. Klicken Sie für die ausgewählte Komponente auf die Schaltfläche **Einstellungen**.

4. Aktivieren Sie auf der Registerkarte **Leistung** im Abschnitt **Untersuchungsmethoden** das Kontrollkästchen **Heuristische Analyse** und stellen Sie darunter die Genauigkeitsstufe ein.

UNTERSUCHUNG OPTIMIEREN

Um die Untersuchungsdauer zu reduzieren und die Arbeitsgeschwindigkeit von Kaspersky Internet Security zu steigern, können Sie festlegen, dass nur neue Dateien und Dateien, die seit ihrer letzten Analyse verändert wurden, untersucht werden. Dieser Modus erstreckt sich auf gewöhnliche und zusammengesetzte Dateien.

- *Gehen Sie folgendermaßen vor, damit nur neue Dateien und Dateien, die seit der letzten Analyse verändert wurden, untersucht werden:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Datei-Anti-Virus** aus.
3. Klicken Sie für die ausgewählte Komponente auf die Schaltfläche **Einstellungen**.
4. Aktivieren Sie auf der Registerkarte **Leistung** im Abschnitt **Untersuchung optimieren** das Kontrollkästchen **Nur neue und veränderte Dateien untersuchen**.

UNTERSUCHUNG VON ZUSAMMENGESETZTEN DATEIEN

Eine häufige Methode zum Verstecken von Viren ist das Eindringen von Schädlingen in zusammengesetzte Dateien wie Archive, Datenbanken usw. Um Viren zu erkennen, die auf diese Weise versteckt wurden, muss eine zusammengesetzte Datei entpackt werden. Dadurch kann das Untersuchungstempo wesentlich sinken.

Installationspakete und Dateien, die OLE-Objekte enthalten, werden beim Öffnen ausgeführt und gelten deshalb als gefährlicher als Archive. Indem die Untersuchung von Archiven deaktiviert und die Untersuchung von Dateien dieser Typen aktiviert wird, schützen Sie Ihren Computer vor der Ausführung von schädlichem Code und senken gleichzeitig die Untersuchungsgeschwindigkeit.

In der Grundeinstellung untersucht Kaspersky Internet Security nur angehängte OLE-Objekte.

- *Gehen Sie folgendermaßen vor, um Liste der zu untersuchenden zusammengesetzten Dateien zu ändern:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Datei-Anti-Virus** aus.
3. Klicken Sie für die ausgewählte Komponente auf die Schaltfläche **Einstellungen**.
4. Aktivieren Sie im folgenden Fenster auf der Registerkarte **Leistung** im Block **Untersuchung von zusammengesetzten Dateien** die Kontrollkästchen der zusammengesetzten Dateien, die vom Programm untersucht werden sollen.

UNTERSUCHUNG UMFANGREICHER ZUSAMMENGESETZTER DATEIEN

Bei der Untersuchung von umfangreichen zusammengesetzten Dateien kann das vorausgehende Entpacken viel Zeit beanspruchen. Die Dauer kann reduziert werden, wenn die Untersuchung von Dateien im Hintergrundmodus erfolgt. Wenn bei der Arbeit mit einer solchen Datei ein schädliches Objekt gefunden wird, werden Sie von Kaspersky Internet Security darüber informiert.

Um die Verzögerung beim Zugriff auf zusammengesetzte Dateien zu reduzieren, kann das Entpacken von Dateien, die eine bestimmte Größe überschreiten, deaktiviert werden. Beim Extrahieren aus Archiven werden Dateien immer untersucht.

- *Gehen Sie folgendermaßen vor, damit Kaspersky Internet Security umfangreiche Dateien im Hintergrundmodus entpackt:*

  1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
  2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Datei-Anti-Virus** aus.
  3. Klicken Sie für die ausgewählte Komponente auf die Schaltfläche **Einstellungen**.
  4. Klicken Sie auf der Registerkarte **Leistung** im Abschnitt **Untersuchung von zusammengesetzten Dateien** auf die Schaltfläche **Erweitert**.
  5. Aktivieren Sie im Fenster **Zusammengesetzte Dateien** das Kontrollkästchen **Zusammengesetzte Dateien im Hintergrund entpacken** und legen Sie im Feld unten die minimale Dateigröße fest.

- *Gehen Sie folgendermaßen vor, damit Kaspersky Internet Security umfangreiche zusammengesetzte Dateien nicht entpackt:*

  1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
  2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Datei-Anti-Virus** aus.
  3. Klicken Sie für die ausgewählte Komponente auf die Schaltfläche **Einstellungen**.
  4. Klicken Sie auf der Registerkarte **Leistung** im Abschnitt **Untersuchung von zusammengesetzten Dateien** auf die Schaltfläche **Erweitert**.
  5. Aktivieren Sie im Fenster **Zusammengesetzte Dateien** das Kontrollkästchen **Große zusammengesetzte Dateien nicht entpacken** und legen Sie im Feld unten einen Wert für die maximale Dateigröße fest.

UNTERSUCHUNGSMODUS ÄNDERN

Unter Untersuchungsmodus wird die Bedingung für das Auslösen von Datei-Anti-Virus verstanden. In der Grundeinstellung verwendet Kaspersky Internet Security den intelligenten Modus, in dem die Entscheidung über die Untersuchung eines Objekts auf Basis der Operationen, die damit ausgeführt werden sollen, gefällt wird. Beispielsweise untersucht Kaspersky Internet Security bei der Arbeit mit einem Microsoft Office-Dokument eine Datei, wenn sie zum ersten Mal geöffnet und zum letzten Mal geschlossen wird. Alle dazwischen liegenden Operationen, bei denen die Datei verändert wird, werden von der Untersuchung ausgeschlossen.

Sie können den Untersuchungsmodus für Objekte ändern. Der passende Modus ist davon abhängig, mit welcher Art von Dateien Sie überwiegend arbeiten.

- *Gehen Sie folgendermaßen vor, um den Untersuchungsmodus für Objekte zu ändern:*

  1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
  2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Datei-Anti-Virus** aus.
  3. Klicken Sie für die ausgewählte Komponente auf die Schaltfläche **Einstellungen**.
  4. Wählen Sie auf der Registerkarte **Erweitert** im Abschnitt **Untersuchungsmodus** den gewünschten Modus.

UNTERSUCHUNGSTECHNOLOGIE

Zusätzlich können Sie die Technologie auswählen, die Datei-Anti-Virus verwenden soll:

- **iChecker**. Eine Technologie, die eine Steigerung der Untersuchungsgeschwindigkeit erlaubt, indem bestimmte Objekte ausgeschlossen werden. Objekte werden nach einem speziellen Algorithmus von der Untersuchung ausgeschlossen. Dabei werden das Erscheinungsdatum der Datenbanken von Kaspersky Internet Security, das Datum der letzten Untersuchung des Objekts und Veränderungen der Untersuchungsparameter berücksichtigt.

  Es kann beispielsweise sein, dass einer Archivdatei aufgrund der Untersuchungsergebnisse der Status *virenfrei* zugewiesen wurde. Dann wird das Archiv von der folgenden Untersuchung ausgeschlossen, wenn es nicht verändert wurde und die Untersuchungsparameter gleich geblieben sind. Wenn die Zusammensetzung des Archivs durch Hinzufügen eines neuen Objekts verändert wurde, die Untersuchungsparameter geändert oder die Datenbanken aktualisiert wurden, wird das Archiv erneut untersucht.

  Die Technologie iChecker besitzt folgende Einschränkungen: Sie funktioniert nicht mit großen Dateien und kann nur auf Objekte angewandt werden, deren Struktur dem Programm bekannt ist (z.B. die Dateiformate *exe*, *dll*, *lnk*, *ttf*, *inf*, *sys*, *com*, *chm*, *zip*, *rar*).

- **iSwift**. Diese Technologie stellt eine Weiterentwicklung der iChecker-Technologie für Computer mit NTFS-Dateisystem dar. Die Technologie iSwift besitzt folgende Einschränkungen: Sie ist an einen konkreten Ort der Datei im Dateisystem gebunden und kann nur auf Objekte angewandt werden, die sich in einem NTFS-Dateisystem befinden.

➡ *Gehen Sie folgendermaßen vor, um die Untersuchungstechnologie für Objekte zu ändern:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.

2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Datei-Anti-Virus** aus.

3. Klicken Sie für die ausgewählte Komponente auf die Schaltfläche **Einstellungen**.

4. Wählen Sie im folgenden Fenster auf der Registerkarte **Erweitert** im Block **Untersuchungstechnologien** den erforderlichen Parameterwert.

KOMPONENTE ANHALTEN: ZEITPLAN ERSTELLEN

Bei der Ausführung von Arbeiten, die die Betriebssystemressourcen stark beanspruchen, können Sie die Arbeit von Datei-Anti-Virus vorübergehend anhalten. Um die Belastung zu verringern und den schnellen Zugriff auf Objekte zu gewährleisten, kann in den Einstellungen festlegt werden, dass die Komponente für einen bestimmten Zeitraum angehalten wird.

Abbildung 7: Rechter Teil des Hauptfensters

➡ *Gehen Sie folgendermaßen vor, um den Zeitplan anzupassen, nach dem eine Komponente angehalten werden soll:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.

2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Datei-Anti-Virus** aus.

3. Klicken Sie für die ausgewählte Komponente auf die Schaltfläche **Einstellungen**.

4. Aktivieren Sie im folgenden Fenster auf der Registrierkarte **Erweitert** im Block **Aufgabe anhalten** das Kontrollkästchen **Nach Zeitplan** und klicken Sie auf die Schaltfläche **Zeitplan**.

5. Geben Sie im Fenster **Aufgabe anhalten** in den Feldern **Anhalten um** und **Fortsetzen um** den erforderlichen Zeitraum an (im Format HH:MM).

KOMPONENTE ANHALTEN: LISTE DER PROGRAMME ERSTELLEN

Bei der Ausführung von Arbeiten, die die Betriebssystemressourcen stark beanspruchen, können Sie die Arbeit von Datei-Anti-Virus vorübergehend anhalten. Um die Belastung zu verringern und den schnellen Zugriff auf Objekte zu gewährleisten, kann in den Einstellungen festlegt werden, dass die Komponente bei der Arbeit mit bestimmten Programmen angehalten wird.

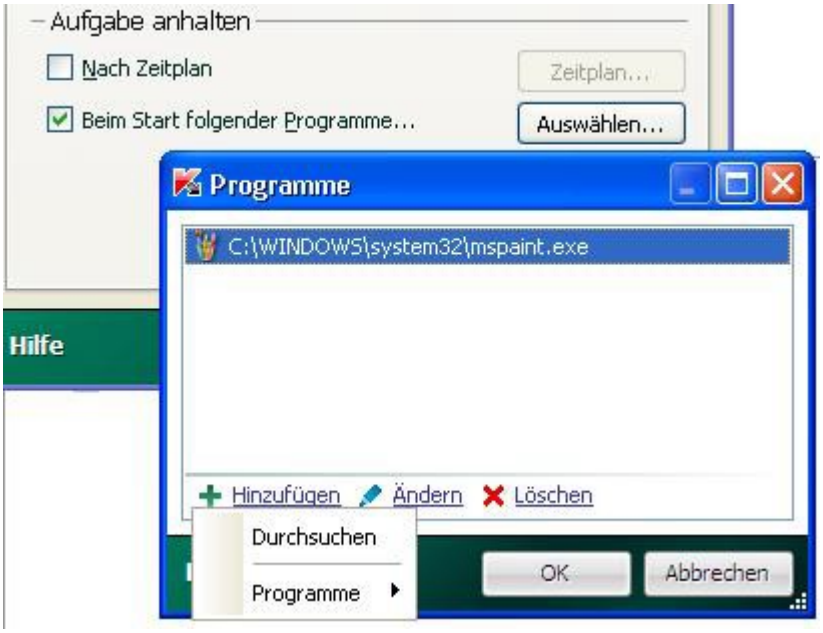

Abbildung 8: Zeitplan erstellen

Das Deaktivieren von Datei-Anti-Virus bei einem Konflikt mit bestimmten Programmen gilt als Notlösung! Sollten bei der Arbeit der Komponente Konflikte auftreten, dann wenden Sie sich an den technischen Support von Kaspersky Lab (http://support.kaspersky.de). Die Spezialisten helfen Ihnen dabei, auf Ihrem Computer die gemeinsame Arbeit von Kaspersky Internet Security mit anderen Programmen einzurichten.

➡ *Gehen Sie folgendermaßen vor, um festzulegen, dass die Komponente angehalten wird, während die angegebenen Programme arbeiten:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.

2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Datei-Anti-Virus** aus.

3. Klicken Sie für die ausgewählte Komponente auf die Schaltfläche **Einstellungen**.

4. Aktivieren Sie im folgenden Fenster auf der Registerkarte **Erweitert** im Block **Aufgabe anhalten** das Kontrollkästchen **Beim Start folgender Programme** und klicken Sie auf die Schaltfläche **Auswählen**.

5. Legen Sie im Fenster **Programme** die Liste der Programme an, bei deren Arbeit die Komponente angehalten werden soll.

STANDARDMÄßIGE SCHUTZPARAMETER WIEDERHERSTELLEN

Während Sie die Arbeit von Datei-Anti-Virus konfigurieren, können Sie jederzeit zu den empfohlenen Einstellungen zurückkehren. Diese gelten als optimal, werden von den Kaspersky-Lab-Spezialisten empfohlen und sind in der Sicherheitsstufe **Empfohlen** zusammengefasst.

Gehen Sie folgendermaßen vor, um die standardmäßigen Schutzeinstellungen wiederherzustellen,

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.

2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Datei-Anti-Virus** aus.

3. Klicken Sie für die ausgewählte Komponente im Block **Sicherheitsstufe** auf die Schaltfläche **Standard**.

E-MAIL-SCHUTZ

Mail-Anti-Virus untersucht, ob in ein- und ausgehenden E-Mails gefährliche Objekte vorhanden sind. Mail-Anti-Virus wird beim Hochfahren des Betriebssystems gestartet, befindet sich ständig im Arbeitsspeicher des Computers und untersucht alle E-Mails der Protokolle POP3, SMTP, IMAP, MAPI und NNTP.

Die E-Mail-Untersuchung erfolgt mit einer bestimmten Auswahl von Parametern, die als Sicherheitsstufe bezeichnet wird. Wenn eine Bedrohung festgestellt wird, führt Mail-Anti-Virus die vorgegebene Aktion (s. Abschnitt "Aktion für gefundene Objekte ändern" auf S. 59) aus. Die Regeln, nach denen die Untersuchung Ihrer Post erfolgt, werden durch eine Anzahl von Parametern bestimmt. Sie lassen sich in Gruppen unterteilen, die folgende Details festlegen:

- geschützter E-Mail-Datenstrom.
- heuristische Analysemethoden verwenden.
- Untersuchung von zusammengesetzten Dateien.
- Filterung angehängter Dateien.

Die Spezialisten von Kaspersky Lab warnen davor, die Funktionsparameter von Mail-Anti-Virus zu verändern. In den meisten Fällen ist es ausreichend, eine andere Sicherheitsstufe auszuwählen. Sie können die Standardeinstellungen von E-Mail-Anti-Virus wiederherstellen. Wählen Sie dazu eine Sicherheitsstufe aus.

➧ *Gehen Sie folgendermaßen vor, um die Funktionsparameter von Mail-Anti-Virus anzupassen:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Mail-Anti-Virus** aus.
3. Klicken Sie für die ausgewählte Komponente auf die Schaltfläche **Einstellungen**.
4. Passen Sie die Parameter der Komponente entsprechend an.

IN DIESEM ABSCHNITT

Algorithmus für die Arbeit der Komponente 58

Sicherheitsstufe für den E-Mail-Schutz ändern 58

Aktion für gefundene Objekte ändern 59

Schutzbereich festlegen 60

E-Mail-Untersuchung in Microsoft Office Outlook 60

E-Mail-Untersuchung in The Bat! 61

Heuristische Analyse verwenden 62

Untersuchung von zusammengesetzten Dateien 62

Anlagenfilterung 62

Standardparameter für den Mail-Schutz wiederherstellen 63

ALGORITHMUS FÜR DIE ARBEIT DER KOMPONENTE

Mail-Anti-Virus ist eine Komponente von Kaspersky Internet Security, die die Untersuchung von E-Mails auf gefährliche Objekte gewährleistet. Diese Komponente wird beim Start des Betriebssystems gestartet, befindet sich ständig im Arbeitsspeicher des Computers und untersucht alle E-Mail-Nachrichten der Protokolle POP3, SMTP, IMAP, MAPI und NNTP, sowie über geschützte Verbindungen (SSL) mit den Protokollen POP3 und IMAP.

Als Indikator für die Arbeit der Komponente dient das Symbol im Infobereich der Taskleiste, das jedes Mal bei der Untersuchung einer E-Mail das Aussehen annimmt.

Der E-Mail-Schutz erfolgt standardmäßig nach folgendem Algorithmus:

1. Jede Nachricht, die vom Benutzer empfangen oder gesendet wird, wird von der Komponente abgefangen.

2. Die E-Mail-Nachricht wird in ihre Bestandteile zerlegt: Kopfzeile, Briefkörper, Anhänge.

3. Der Körper und die Anhänge der E-Mail-Nachricht (einschließlich eingebetteten OLE-Objekten) werden auf gefährliche Objekte untersucht. Schädliche Objekte werden auf Basis der Datenbanken erkannt, die bei der Arbeit von Kaspersky Internet Security verwendet werden, sowie mit Hilfe eines heuristischen Algorithmus. Die Datenbanken enthalten eine Beschreibung aller momentan bekannten schädlichen Programme und Methoden zu deren Desinfektion. Der heuristische Algorithmus erlaubt es, neue Viren zu erkennen, die noch nicht in den Datenbanken beschrieben sind.

4. Aufgrund der Virenuntersuchung bestehen folgende Varianten für das weitere Vorgehen:

   - Wenn der Körper oder ein Anhang der Nachricht schädlichen Code enthält, sperrt der Schutz für E-Mails und Instant-Messenger die E-Mail, speichert eine Sicherungskopie davon im Backup und versucht das Objekt zu desinfizieren. Bei erfolgreicher Desinfektion erhält der Benutzer Zugriff auf die E-Mail. Wenn die Desinfektion fehlschlägt, wird das infizierte Objekt aus der Nachricht gelöscht. Als Ergebnis der Antiviren-Bearbeitung wird in die Betreffzeile der E-Mail ein spezieller Text eingefügt, der darüber informiert, dass sie von Kaspersky Internet Security bearbeitet wurde.

   - Wenn der Körper oder ein Anhang der Nachricht einen Code enthält, der Ähnlichkeit mit schädlichem Code besitzt, jedoch keine hundertprozentige Sicherheit darüber besteht, wird der verdächtige Teil der Nachricht in die Quarantäne verschoben.

   - Wenn in der E-Mail kein schädlicher Code gefunden wird, erhält der Benutzer sofort Zugriff darauf.

Für das Mailprogramm Microsoft Office Outlook ist ein integrierbares Erweiterungsmodul (s. Abschnitt "E-Mail-Untersuchung in Microsoft Office Outlook" auf S. 60) vorgesehen, mit dem die Untersuchung von E-Mails feiner eingestellt werden kann.

Wenn Sie das Mailprogramm The Bat! verwenden, kann Kaspersky Internet Security zusammen mit anderen Antiviren-Anwendungen benutzt werden. Dabei werden die Regeln zur Verarbeitung des Mailverkehr (s. Abschnitt "E-Mail-Untersuchung in The Bat!" auf S. 61) direkt in The Bat! eingestellt und haben Vorrang vor den Parametern für den E-Mail durch die Anwendung.

Bei der Arbeit mit anderen Mailprogrammen (einschließlich Microsoft Outlook Express (Windows Mail), Mozilla Thunderbird, Eudora, IncrediMail) untersucht Mail-Anti-Virus den Mailverkehr der Protokolle SMTP, POP3, IMAP und NNTP bei Empfang bzw. Versand.

Beachten Sie, dass bei der Arbeit mit dem Mailprogramm Thunderbird E-Mails, die mit dem IMAP- Protokoll übertragen werden, nicht auf Viren untersucht werden, wenn Filter verwendet werden, die Nachrichten aus dem Ordner **Posteingang** verschieben.

SICHERHEITSSTUFE FÜR DEN E-MAIL-SCHUTZ ÄNDERN

Unter Sicherheitsstufe wird eine vordefinierte Auswahl von Parametern für Mail-Anti-Virus verstanden. Die Spezialisten von Kaspersky Lab haben drei Sicherheitsstufen vordefiniert. Sie treffen selbst eine Entscheidung über die Auswahl der

Sicherheitsstufe, wobei die Arbeitsbedingungen und die aktuelle Situation berücksichtigt werden sollten. Folgende Sicherheitsstufen stehen zur Auswahl:

- **Hoch**. Wenn Sie in einer gefährlichen Umgebung arbeiten, ist die maximale Sicherheitsstufe geeignet. Als Beispiel für eine gefährliche Umgebung kann eine Verbindung des Computers mit einem kostenlosen Mailanbieter dienen, wenn die Verbindung aus einem lokalen Netzwerk erfolgt, das nicht über einen zentralisierten E-Mail-Schutz verfügt.

- **Empfohlen**. Diese Stufe bietet ein ausgewogenes Verhältnis zwischen Leistung und Sicherheit. Sie ist für die meisten Situationen geeignet. Die empfohlene Stufe entspricht der Grundeinstellung.

- **Niedrig**. Wenn Sie in einer gut geschützten Umgebung arbeiten, ist die niedrige Sicherheitsstufe geeignet. Als Beispiel für eine solche Umgebung kann ein Firmennetzwerk mit zentralisiertem E-Mail-Schutz dienen.

Wenn keine vordefinierte Stufe Ihren Anforderungen entspricht, können Sie die Einstellungen (s. Abschnitt "Schutz für E-Mail" auf S. 57) von Mail-Anti-Virus anpassen. Dadurch ändert sich der Name der Sicherheitsstufe in **Benutzerdefiniert**. Um die standardmäßigen Einstellungen der Komponente wiederherzustellen, wählen Sie eine der vordefinierten Stufen aus.

➡ *Gehen Sie folgendermaßen vor, um die festgelegte Sicherheitsstufe für E-Mails zu ändern:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.

2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Mail-Anti-Virus** aus.

3. Legen Sie die erforderliche Sicherheitsstufe für die gewählte Komponente fest.

AKTION FÜR GEFUNDENE OBJEKTE ÄNDERN

Mail-Anti-Virus untersucht E-Mail-Nachrichten. Wenn sich durch die Virenuntersuchung ergibt, dass eine E-Mail oder ein E-Mail-Objekt (Briefkörper, Anhang) infiziert oder möglicherweise infiziert ist, sind die weiteren Operationen, die die Komponente ausführt, vom Status des Objekts und von der ausgewählten Aktion abhängig.

Mail-Anti-Virus weist gefundenen Objekten aufgrund des Untersuchungsergebnisses einen der folgenden Status zu:

- Status eines der schädlichen Programme (beispielsweise *Virus*, *trojanisches Programm*).

- Status *möglicherweise infiziert*, wenn sich aufgrund der Untersuchung nicht eindeutig feststellen lässt, ob das Objekt infiziert ist oder nicht. Das bedeutet, dass in der E-Mail oder in einem E-Mail-Objekt die Codefolge eines unbekannten Virus oder der modifizierte Code eines bekannten Virus gefunden wurde.

Wenn Kaspersky Internet Security bei einer E-Mail-Untersuchung infizierte oder möglicherweise infizierte Objekte findet, werden Sie darüber informiert. Sie werden dazu aufgefordert, auf die gefundene Bedrohung zu reagieren, indem Sie eine Aktion für das Objekt auswählen. Standardmäßig ist in Kaspersky Internet Security als Aktion für ein gefundenes Objekt die Variante **Aktion erfragen** festgelegt. Sie können die Aktion ändern. Wenn Sie beispielsweise sicher sind, dass versucht werden soll, alle gefundenen Objekte zu desinfizieren, und bei einer Meldung über den Fund eines infizierten oder verdächtigen Objekts in einer E-Mail nicht jedes Mal die Aktion **Desinfizieren** auswählen möchten, dann legen Sie folgende Aktion fest: **Aktion ausführen. Desinfizieren**.

Bevor ein infiziertes Objekt desinfiziert oder gelöscht wird, legt Kaspersky Internet Security eine Sicherungskopie des Objekts an. Dadurch wird erlaubt, das Objekt bei Bedarf wiederherzustellen oder später zu desinfizieren.

Wenn Sie im automatischen Modus (s. Abschnitt "Schritt 2. Schutzmodus auswählen" auf S. 32) arbeiten, wendet Kaspersky Internet Security automatisch die von den Kaspersky-Lab-Fachleuten empfohlene Aktion an, wenn gefährliche Objekte erkannt werden. Für schädliche Objekte ist dies die Aktion **Desinfizieren. Löschen, wenn Desinfektion nicht möglich**, für verdächtige – **Überspringen**.

- *Gehen Sie folgendermaßen vor, um die festgelegte Aktion für gefundene Objekte zu ändern:*

  1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
  2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Mail-Anti-Virus** aus.
  3. Geben Sie die entsprechende Aktion für die gewählte Komponente an.

SCHUTZBEREICH FESTLEGEN

Unter Schutzbereich wird der Typ der Nachrichten verstanden, die untersucht werden sollen. Standardmäßig untersucht Kaspersky Internet Security sowohl eingehende, als auch ausgehende E-Mails. Wenn Sie nur die Untersuchung eingehender E-Mails gewählt haben, ist es empfehlenswert, zu Beginn der Arbeit mit Kaspersky Internet Security die ausgehenden E-Mails zu untersuchen, weil sich auf Ihrem Computer Mailwürmer befinden können, die E-Mails als Kanal verwenden, um sich weiterzuverbreiten. Dadurch wird erlaubt, Probleme zu verhindern, die mit dem unkontrollierten Versenden infizierter E-Mails von Ihrem Computer verbunden sind.

Zum Schutzbereich gehören auch die Parameter für die Integration von Mail-Anti-Virus in das System und die zu untersuchenden Protokolle. In der Grundeinstellung wird Mail-Anti-Virus in die Mailprogramme Microsoft Office Outlook und The Bat! integriert.

- *Gehen Sie folgendermaßen vor, um die Untersuchung ausgehender E-Mails auszuschalten:*

  1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
  2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Mail-Anti-Virus** aus.
  3. Klicken Sie für die ausgewählte Komponente auf die Schaltfläche **Einstellungen**.
  4. Geben Sie im folgenden Fenster Registerkarte **Allgemein** im Block **Schutzbereich** die gewünschten Parameterwerte an.

- *Gehen Sie folgendermaßen vor, um die zu untersuchenden Protokolle und die Parameter für die Integration von Mail-Anti-Virus in das System festzulegen:*

  1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
  2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Mail-Anti-Virus** aus.
  3. Klicken Sie für die ausgewählte Komponente auf die Schaltfläche **Einstellungen**.
  4. Wählen Sie im folgenden Fenster auf der Registerkarte **Erweitert** im Block **Integration ins System** die erforderlichen Parameter.

E-MAIL-UNTERSUCHUNG IN MICROSOFT OFFICE OUTLOOK

Wenn Microsoft Office Outlook als Mailprogramm verwendet wird, können Sie die Virenuntersuchung Ihrer E-Mails zusätzlich anpassen.

Bei der Installation von Kaspersky Internet Security wird ein spezielles Erweiterungsmodul in Microsoft Office Outlook integriert. Es erlaubt Ihnen, schnell zu den Einstellungen von Mail-Anti-Virus zu wechseln und festzulegen, wann eine E-Mail-Nachricht auf das Vorhandensein gefährlicher Objekte untersucht werden soll.

Das Erweiterungsmodul besitzt die Form einer speziellen Registerkarte mit dem Namen **E-Mail-Schutz**, die sich im Menü **Extras** → Optionen befindet. Auf der Registerkarte können Sie die Untersuchungsmodi für E-Mail festlegen.

➡ *Gehen Sie folgendermaßen vor, um den Untersuchungsmodus für E-Mails festzulegen:*

1. Öffnen Sie das Hauptfenster von Microsoft Office Outlook.
2. Wählen Sie im Programmmenü den Punkt **Extras** → **Optionen**.
3. Legen Sie auf der Registerkarte **E-Mail-Schutz** den erforderlichen Modus für die E-Mail-Untersuchung fest.

E-MAIL-UNTERSUCHUNG IN THE BAT!

Die Aktionen für infizierte E-Mail-Objekte werden durch das Mailprogramm The Bat! selbst festgelegt.

Die Parameter von Mail-Anti-Virus, die festlegen, ob ein- und ausgehende E-Mails untersucht werden, und die Aktionen für gefährliche E-Mail-Objekte und Ausnahmen bestimmen, werden ignoriert. Das Programm The Bat! berücksichtigt lediglich die Untersuchung angehängter Archive.

Die hier angezeigten Parameter für den E-Mail-Schutz gelten für alle auf dem Computer installierten Antiviren-Module, die die Arbeit mit The Bat! unterstützen.

Es sollte beachtet werden, dass E-Mails beim Empfang zuerst von Mail-Anti-Virus untersucht werden und erst anschließend von dem Plug-in des Mailprogramms The Bat!. Wenn ein schädliches Objekt gefunden wird, werden Sie von Kaspersky Internet Security auf jeden Fall darüber informiert. Wenn dabei im Meldungsfenster von Mail-Anti-Virus die Aktion **Desinfizieren** (**Löschen**) gewählt wird, führt Mail-Anti-Virus das Löschen der Bedrohung aus. Wird im Meldungsfenster die Aktion **Überspringen** gewählt, so wird das Objekt von dem Plug-in für The Bat! desinfiziert. Beim Senden werden E-Mails zuerst von dem Plug-in und anschließend von Mail-Anti-Virus untersucht.

Folgende Einstellungen sind erforderlich:

- Welche Richtung des E-Mail-Verkehrs (eingehende, ausgehende) der Untersuchung unterzogen werden soll.
- Wann die Untersuchung von E-Mail-Objekten erfolgen soll (beim Öffnen einer E-Mail oder vor dem Speichern auf der Festplatte).
- Aktionen, die das Mailprogramm ausführen soll, wenn gefährliche Objekte in E-Mails gefunden werden. Es stehen beispielsweise zur Auswahl:
  - **Reparaturversuch infizierter Teile** – Bei Auswahl dieser Variante wird versucht, ein infiziertes Objekt zu desinfizieren. Wenn die Desinfektion fehlschlägt, verbleibt das Objekt in der Nachricht.
  - **Infizierte Teile löschen** – Bei Auswahl dieser Variante wird ein gefährliches E-Mail-Objekt gelöscht. Dabei bleibt unberücksichtigt, ob es infiziert ist oder als verdächtig gilt.

Standardmäßig verschiebt das Programm The Bat! alle infizierten E-Mail-Objekte ohne Desinfektion in die Quarantäne.

E-Mail-Nachrichten, die gefährliche Objekte enthalten, werden von dem Programm The Bat! nicht durch eine spezielle Kopfzeile gekennzeichnet.

➡ *Gehen Sie folgendermaßen vor, um in The Bat! die Einstellungen für den E-Mail-Schutz anzupassen:*

1. Öffnen Sie das Hauptfenster von The Bat!.
2. Wählen Sie im Menü **Optionen** des Mailprogramms den Punkt **Benutzereinstellungen**.
3. Wählen Sie in der Konfigurationsstruktur den Punkt **Anti-Virus-Plug-Ins**.

HEURISTISCHE ANALYSE VERWENDEN

Die heuristische Methode besteht in der Analyse der Aktivität, die ein Objekt im System zeigt. Wenn diese Aktivität als typisch für schädliche Objekte gilt, lässt sich ein Objekt mit hoher Wahrscheinlichkeit als schädlich oder verdächtig einstufen. Dadurch können neue Bedrohungen bereits erkannt werden, bevor die Virenanalytiker von ihrer Aktivität wissen. In der Grundeinstellung ist die heuristische Analyse aktiviert.

Kaspersky Internet Security informiert Sie darüber, wenn in einer Nachricht ein schädliches Objekt gefunden wird. Die Meldung erfordert die Auswahl einer Aktion.

Zusätzlich können Sie das Genauigkeitsniveau der Untersuchung festlegen: **oberflächlich**, **mittel** oder **tief**. Bewegen Sie dazu den Schieberegler auf die gewünschte Position.

- *Gehen Sie folgendermaßen vor, um die heuristische Analyse zu verwenden / zu deaktivieren und die Genauigkeitsstufe der Untersuchung festzulegen:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Mail-Anti-Virus** aus.
3. Klicken Sie für die ausgewählte Komponente auf die Schaltfläche **Einstellungen**.
4. Aktivieren / deaktivieren Sie im folgenden Fenster auf der Registerkarte **Allgemein** im Block **Untersuchungsmethoden** das Kontrollkästchen **Heuristische Analyse** und stellen Sie darunter das Genauigkeitsniveau ein.

UNTERSUCHUNG VON ZUSAMMENGESETZTEN DATEIEN

Die Auswahl des Untersuchungsmodus für zusammengesetzte Dateien beeinflusst die Leistung von Kaspersky Internet Security. Sie können die Untersuchung angehängter Archive aktivieren oder deaktivieren, sowie die maximale Größe der zu untersuchenden Archive begrenzen.

- *Gehen Sie folgendermaßen vor, um die Untersuchungsparameter für zusammengesetzte Dateien anzupassen:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Mail-Anti-Virus** aus.
3. Klicken Sie für die ausgewählte Komponente auf die Schaltfläche **Einstellungen**.
4. Wählen Sie im folgenden Fenster auf der Registerkarte **Allgemein** den Untersuchungsmodus für zusammengesetzte Dateien.

ANLAGENFILTERUNG

Sie können die Filterbedingungen für an E-Mails angehängte Objekte anpassen. Die Verwendung des Filters bietet Ihrem Computer zusätzliche Sicherheit, da sich in E-Mails enthaltene Malware meist in angehängten Dateien befindet. Das Umbenennen oder Löschen von Attachments eines bestimmten Typs erlaubt es, Ihren Computer beispielsweise davor zu schützen, dass eine angehängte Datei beim Empfang einer Nachricht automatisch geöffnet wird.

Wenn Ihr Computer nicht durch die Mittel eines lokalen Netzwerks geschützt ist (die Internetverbindung erfolgt ohne Proxyserver oder Firewall), wird davor gewarnt, die Untersuchung angehängter Archive zu deaktivieren.

Gehen Sie folgendermaßen vor, um die Parameter für die Anlagenfilterung anzupassen:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.

2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Mail-Anti-Virus** aus.

3. Klicken Sie für die ausgewählte Komponente auf die Schaltfläche **Einstellungen**.

4. Legen Sie im folgenden Fenster auf der Registerkarte **Anlagenfilterung** die Bedingungen für die Filterung von Objekten fest, die an E-Mails angehängt sind. Bei Auswahl der letzten beiden Modi wird die Liste der Dateitypen aktiviert. In dieser Liste können Sie die erforderlichen Typen ankreuzen oder die Maske eines neuen Typs hinzufügen.

   Wenn ein neuer Maskentyp hinzugefügt werden soll, klicken Sie auf den Link **Hinzufügen** und geben Sie im folgenden Fenster **Maske für Dateinamen** die erforderlichen Daten ein.

STANDARDPARAMETER FÜR DEN MAIL-SCHUTZ WIEDERHERSTELLEN

Während Sie die Arbeit von Mail-Anti-Virus anpassen, können Sie jederzeit zu den empfohlenen Einstellungen zurückkehren. Diese gelten als optimal, werden von den Kaspersky-Lab-Spezialisten empfohlen und sind in der Sicherheitsstufe **Empfohlen** zusammengefasst.

Gehen Sie folgendermaßen vor, um die standardmäßigen Einstellungen für den Mail-Schutz wiederherzustellen,

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.

2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Mail-Anti-Virus** aus.

3. Klicken Sie für die ausgewählte Komponente im Block **Sicherheitsstufe** auf die Schaltfläche **Standard**.

SCHUTZ FÜR WEB-DATENVERKEHR

Immer wenn Sie im Internet arbeiten, besteht für die Informationen, die auf Ihrem Computer gespeichert sind, das Risiko einer Infektion durch gefährliche Programme. Sie können in Ihren Computer eindringen, während Sie kostenlose Programme herunterladen oder scheinbar ungefährliche Seiten besuchen (die zuvor von Hackern angegriffen wurden). Außerdem können Netzwürmer direkt beim Aufbau einer Internetverbindung in Ihren Computer eindringen, bevor überhaupt eine Webseite geöffnet oder eine Datei heruntergeladen wird.

Die Sicherheit Ihrer Arbeit im Internet wird von der Komponente *Web-Anti-Virus* gewährleistet. Er schützt Informationen, die über das HTTP-Protokoll auf Ihren Computer gelangen, und verhindert den Start gefährlicher Skripts auf Ihrem Computer.

Der Web-Schutz sieht nur die Kontrolle des HTTP-Datenverkehrs vor, der über die Ports, die in der Liste zu kontrollierenden Ports angegeben sind, übertragen wird. Eine Liste der Ports, die am häufigsten zur Übertragung von E-Mails und HTTP-Datenverkehr benutzt werden, ist im Lieferumfang von Kaspersky Internet Security enthalten. Wenn Sie Ports verwenden, die nicht zu dieser Liste gehören, sollten diese der Liste hinzugefügt werden, um den Schutz des über sie abgewickelten Datenverkehrs zu gewährleisten.

Wenn Sie in einer ungeschützten Umgebung arbeiten, ist es empfehlenswert, bei der Arbeit im Internet die Komponente Web-Anti-Virus zu verwenden. Wenn Ihr Computer in einem Netzwerk arbeitet, das durch eine Firewall oder durch HTTP-Traffic-Filter gesichert ist, gewährleistet Web-Anti-Virus dem Computer zusätzliche Sicherheit.

Die Untersuchung des Datenverkehrs erfolgt mit einer bestimmten Auswahl von Parametern, die als Sicherheitsstufe bezeichnet wird. Beim Fund von Bedrohungen führt Web-Anti-Virus die festgelegte Aktion aus.

Das Schutzniveau, das auf Ihrem Computer für den Web-Datenverkehr gilt, wird durch eine Auswahl von Parametern festgelegt. Sie lassen sich in folgende Gruppen aufteilen:

- Parameter, die den Schutzbereich definieren.
- Parameter, die die Leistung des Schutzes für den Datenverkehr (Heuristische Analyse verwenden, Untersuchung optimieren) festlegen.

Die Spezialisten von Kaspersky Lab warnen davor, die Funktionsparameter von Web-Anti-Virus zu verändern. In den meisten Fällen ist es ausreichend, eine andere Sicherheitsstufe auszuwählen.

➡ *Gehen Sie folgendermaßen vor, um die Funktionsparameter von Web-Anti-Virus anzupassen:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Web-Anti-Virus** aus.
3. Klicken Sie für die ausgewählte Komponente auf die Schaltfläche **Einstellungen**.
4. Passen Sie die Parameter der Komponente entsprechend an.

IN DIESEM ABSCHNITT

Algorithmus für die Arbeit der Komponente 65

Sicherheitsstufe für den HTTP-Datenverkehr ändern 66

Aktion für gefundene Objekte ändern 66

Schutzbereich festlegen 67

Untersuchungstyp auswählen 67

Modul zur Link-Untersuchung 68

Heuristische Analyse verwenden 69

Untersuchung optimieren 69

Standardparameter für den Web-Schutz wiederherstellen 70

ALGORITHMUS FÜR DIE ARBEIT DER KOMPONENTE

Web-Anti-Virus schützt Informationen, die über das HTTP-Protokoll auf Ihren Computer gelangen, und verhindert auf Ihrem Computer den Start gefährlicher Skripts.

Im Folgenden wird das Funktionsschema der Komponente näher beschrieben. Der Schutz des HTTP-Verkehrs erfolgt nach folgendem Algorithmus:

1. Jede Webseite oder Datei, auf die ein Benutzer oder ein bestimmtes Programm über das HTTP-Protokoll zugreift, wird von Web-Anti-Virus abgefangen und auf schädlichen Code analysiert. Die Suche nach schädlichen Objekten erfolgt auf Basis der Datenbanken, die bei der Arbeit von Kaspersky Internet Security verwendet werden, sowie mit Hilfe eines heuristischen Algorithmus. Die Datenbanken enthalten eine Beschreibung aller momentan bekannten schädlichen Programme und Methoden zu deren Desinfektion. Der heuristische Algorithmus erlaubt es, neue Viren zu erkennen, die noch nicht in den Datenbanken beschrieben sind.

2. Aufgrund der Virenuntersuchung bestehen folgende Varianten für das weitere Vorgehen:

   - Wenn eine Webseite oder ein Objekt, auf das ein Benutzer zugreift, schädlichen Code enthält, wird der Zugriff darauf blockiert. Dabei erscheint auf dem Bildschirm eine Meldung darüber, dass das angeforderte Objekt oder die Seite infiziert ist.

   - Wenn die Datei oder Webseite keinen schädlichen Code enthält, erhält der Benutzer sofort Zugriff darauf.

Die Untersuchung von Skripts wird nach folgendem Algorithmus ausgeführt:

1. Jedes auf einer Webseite auszuführende Skript wird von Web-Anti-Virus abgefangen und auf schädlichen Code analysiert.

2. Wenn ein Skript schädlichen Code enthält, wird es von Web-Anti-Virus gesperrt und der Benutzer wird durch eine spezielle Popupmeldung benachrichtigt.

3. Wenn im Skript kein schädlicher Code gefunden wird, wird es ausgeführt.

Skripts werden nur auf Webseiten abgefangen, die mit Microsoft Internet Explorer gestartet werden.

SICHERHEITSSTUFE FÜR DEN HTTP-DATENVERKEHR ÄNDERN

Unter Sicherheitsstufe wird eine vordefinierte Auswahl von Parametern für Web-Anti-Virus verstanden. Die Spezialisten von Kaspersky Lab haben drei Sicherheitsstufen vordefiniert. Sie treffen selbst eine Entscheidung über die Auswahl der Sicherheitsstufe, wobei die Arbeitsbedingungen und die aktuelle Situation berücksichtigt werden sollten. Für die Sicherheitsstufe stehen folgende Varianten zur Auswahl:

- **Hoch**. Es wird empfohlen, diese Stufe in einer aggressiven Umgebung zu verwenden, wenn keine anderen Mittel zum Schutz des HTTP-Datenverkehrs eingesetzt werden.
- **Empfohlen**. Diese Sicherheitsstufe gilt für die meisten Situationen als optimal.
- **Niedrig**. Verwenden Sie diese Sicherheitsstufe, wenn auf Ihrem Computer zusätzliche Mittel zum Schutz des HTTP-Datenverkehrs installiert sind.

Wenn keine vordefinierte Stufe Ihren Anforderungen entspricht, können Sie die Einstellungen (s. Abschnitt "Schutz für Web-Datenverkehr" auf S. 64) von Web-Anti-Virus anpassen. Dadurch ändert sich der Name der Sicherheitsstufe in **Benutzerdefiniert**. Um die standardmäßigen Einstellungen der Komponente wiederherzustellen, wählen Sie eine der vordefinierten Stufen aus.

Gehen Sie folgendermaßen vor, um die festgelegte Sicherheitsstufe für den Web-Datenverkehr zu ändern:

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Web-Anti-Virus** aus.
3. Legen Sie die erforderliche Sicherheitsstufe für die gewählte Komponente fest.

AKTION FÜR GEFUNDENE OBJEKTE ÄNDERN

Wenn sich bei der Analyse eines Objekts des HTTP-Verkehrs herausstellt, dass das Objekt schädlichen Code enthält, sind die weiteren Operationen, die Web-Anti-Virus ausführt, von der Aktion abhängig, die Sie festgelegt haben.

Was die Aktionen für gefährliche Skripts betrifft, so sperrt Web-Anti-Virus deren Ausführung immer und zeigt auf dem Bildschirm eine Popupmeldung an, die den Benutzer über die ausgeführte Aktion informiert. Die Aktion für das gefährliche Objekt kann nicht geändert werden, es kann nur das Modul für die Skript-Untersuchung ausgeschaltet werden (s. Abschnitt "Untersuchungstyp auswählen" auf S. 67).

Wenn Sie im automatischen Modus (s. Abschnitt "Schritt 2. Schutzmodus auswählen" auf S. 32) arbeiten, wendet Kaspersky Internet Security automatisch die von den Kaspersky-Lab-Fachleuten empfohlene Aktion an, wenn gefährliche Objekte erkannt werden.

Gehen Sie folgendermaßen vor, um die festgelegte Aktion für gefundene Objekte zu ändern:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Web-Anti-Virus** aus.
3. Geben Sie die entsprechende Aktion für die gewählte Komponente an.

SCHUTZBEREICH FESTLEGEN

Das Festlegen des Schutzbereichs umfasst die Auswahl des von Web-Anti-Virus verwendeten Untersuchungstyps für Objekte (s. Abschnitt "Untersuchungstyp auswählen" auf S. 67) und das Anlegen einer Liste mit vertrauenswürdigen Webadressen, deren Informationen von der Komponente nicht auf Viren analysiert werden sollen.

Sie können eine Liste der vertrauenswürdigen Webadressen anlegen, deren Inhalt Sie vorbehaltlos vertrauen. Web-Anti-Virus wird die Informationen von diesen Adressen nicht auf gefährliche Objekte hin analysieren. Diese Option kann benutzt werden, wenn Web-Anti-Virus das Laden einer bestimmten Datei verhindert, indem er den Downloadversuch blockiert.

➡ *Gehen Sie folgendermaßen vor, um eine Liste mit vertrauenswürdigen Adressen anzulegen:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.

2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Web-Anti-Virus** aus.

3. Klicken Sie für die ausgewählte Komponente auf die Schaltfläche **Einstellungen**.

4. Aktivieren Sie im folgenden Fenster **Web-Anti-Virus** im Block **Untersuchung optimieren** das Kontrollkästchen ☑ **HTTP-Datenverkehr von vertrauenswürdigen Webadressen nicht untersuchen** und klicken Sie auf die Schaltfläche **Auswählen**.

5. Klicken Sie im folgenden Fenster **Liste der vertrauenswürdigen Webadressen** auf den Link **Hinzufügen**.

6. Geben Sie im folgenden Fenster **Adressenmaske (URL)** eine vertrauenswürdige Adresse (oder ihre Maske) ein.

UNTERSUCHUNGSTYP AUSWÄHLEN

Die Aufgabe Schutzbereich festlegen (s. S. 67) umfasst neben dem Anlegen einer Liste der vertrauenswürdigen Webadressen auch die Auswahl des von Web-Anti-Virus für den Datenverkehr verwendeten Untersuchungstyps. Es wird unterschieden zwischen der Untersuchung von Skripts und der Untersuchung des HTTP-Datenverkehrs.

In der Grundeinstellung führt Web-Anti-Virus gleichzeitig die Untersuchung von HTTP-Datenverkehr und Skripts aus.

Zur Untersuchung des HTTP-Datenverkehrs gehört nicht nur die Untersuchung auf Viren, sondern auch die Untersuchung von Links auf deren Zugehörigkeit zur Liste der verdächtigen Webadressen und / oder zur Liste der Phishing-Webadressen.

Durch die Untersuchung von Links auf die Zugehörigkeit zur Liste der Phishing-Adressen lassen sich Phishing-Angriffe abwehren, die in der Regel die Form von E-Mails besitzen, die scheinbar von finanziellen Strukturen stammen und Links auf deren Webseiten enthalten. Die Nachricht fordert dazu auf, einem Link zu folgen und auf der betreffenden Seite vertrauliche Informationen wie beispielsweise eine Kreditkartennummer oder Benutzername und Kennwort für die persönliche Internet-Banking-Seite einzugeben, auf der finanzielle Operationen erfolgen können.

Da Links, die auf Phishing-Seiten verweisen, nicht nur mit E-Mails, sondern auch mit anderen Mitteln (beispielsweise im Text einer ICQ-Nachricht) an Sie geschickt werden können, überwacht und blockiert die Komponente Web-Anti-Virus alle Versuche zum Öffnen einer Phishing-Seite auf der Ebene des HTTP-Datenverkehrs.

Die Untersuchung von Links auf ihre Zugehörigkeit zur Liste der verdächtigen Webadressen bietet die Kontrolle über Webseiten, die auf der schwarzen Liste stehen. Die Liste wird von den Kaspersky-Lab-Fachleuten angelegt und gehört zum Lieferumfang des Programms.

➡ *Gehen Sie folgendermaßen vor, damit Web-Anti-Virus Skripts untersucht:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.

2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Web-Anti-Virus** aus.

3. Klicken Sie für die ausgewählte Komponente auf die Schaltfläche **Einstellungen**.

4. Vergewissern Sie sich im folgenden Fenster **Web-Anti-Virus** im Block **Erweitert**, dass das Kontrollkästchen **Gefährliche Skripts in Microsoft Internet Explorer blockieren** aktiviert ist. In diesem Fall wird Web-Anti-Virus alle Skripts, die in Microsoft Internet Explorer verarbeitet werden, und alle WSH-Skripts (JavaScript, Visual Basic Script u.a.), die bei der Arbeit eines Benutzers auf dem Computer gestartet werden, untersuchen.

   Außerdem können Sie das Modul Link-Untersuchung verwenden (s. S. 68). Dazu aktivieren Sie das Kontrollkästchen **Phishing-Links und verdächtige Links im Microsoft Internet Explorer und Mozilla Firefox kennzeichnen**. Web-Anti-Virus markiert gefundene Phishing-Links und verdächtige Links in den Webadressen der Browser (Microsoft Internet Explorer und Mozilla Firefox).

Gehen Sie folgendermaßen vor, um Links mit der Datenbank für verdächtige Webadressen und / oder Phishing-Webadressen zu untersuchen:

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.

2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Web-Anti-Virus** aus.

3. Klicken Sie für die ausgewählte Komponente auf die Schaltfläche **Einstellungen**.

4. Vergewissern Sie sich, dass im folgenden Fenster **Web-Anti-Virus** im Block **Untersuchungsmethoden** das Kontrollkästchen **Links mit der Datenbank für verdächtige Webadressen** untersuchen und / oder das Kontrollkästchen **Links mit der Datenbank für Phishing-Webadressen untersuchen** aktiviert ist.

MODUL ZUR LINK-UNTERSUCHUNG

Kaspersky Internet Security umfasst ein Modul zur Link-Untersuchung, das zu der Komponente Web-Anti-Virus gehört. Das Modul untersucht alle Links, die auf einer Webseite vorhanden sind, auf Zugehörigkeit zu verdächtigen und Phishing-Webadressen. Sie können folgende Listen anlegen: eine Liste mit vertrauenswürdigen Adressen von Webseiten, deren Inhalt nicht untersucht werden soll, und eine Liste mit Adressen von Webseiten, deren Inhalt untersucht werden soll. Das Modul wird als Plug-in in die Webbrowser Microsoft Internet Explorer und Mozilla Firefox integriert.

Gehen Sie folgendermaßen vor, um das Modul zur Link-Untersuchung zu aktivieren:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.

2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Web-Anti-Virus** aus.

3. Klicken Sie für die ausgewählte Komponente im Block **Sicherheitsstufe** auf die Schaltfläche **Einstellungen**.

4. Im folgenden Fenster **Web-Anti-Virus** aktivieren Sie im Block **Erweitert** das Kontrollkästchen **Phishing-Links und verdächtige Links im Microsoft Internet Explorer und Mozilla Firefox kennzeichnen**.

Gehen Sie folgendermaßen vor, um eine Liste mit vertrauenswürdigen Adressen anzulegen:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.

2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Web-Anti-Virus** aus.

3. Klicken Sie für die ausgewählte Komponente im Block **Sicherheitsstufe** auf die Schaltfläche **Einstellungen**.

4. Klicken Sie im folgenden Fenster **Web-Anti-Virus** im Block **Erweitert** auf die Schaltfläche **Einstellungen**.

5. Wählen Sie im folgenden Fenster **Modul zur Link-Untersuchung** die Variante **Für alle Webadressen** aus und klicken Sie auf die Schaltfläche **Ausnahmen**.

6. Klicken Sie im folgenden Fenster **Liste der vertrauenswürdigen Webadressen** auf den Link **Hinzufügen**.

7. Geben Sie im folgenden Fenster **Adressenmaske (URL)** eine vertrauenswürdige Adresse (oder ihre Maske) ein.

Gehen Sie folgendermaßen vor, um eine Liste der Webadressen von Seiten anzulegen, deren Inhalt untersucht werden soll:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.

2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Web-Anti-Virus** aus.

3. Klicken Sie für die ausgewählte Komponente im Block **Sicherheitsstufe** auf die Schaltfläche **Einstellungen**.

4. Klicken Sie im folgenden Fenster **Web-Anti-Virus** im Block **Erweitert** auf die Schaltfläche **Einstellungen**.

5. Im folgenden Fenster **Modul zur Link-Untersuchung** wählen Sie auf die Variante **Für die angegebenen Webadressen** aus und klicken Sie auf die Schaltfläche **Auswählen**.

6. Klicken Sie im folgenden Fenster **Liste der zu untersuchenden Webadressen** auf den Link **Hinzufügen**.

7. Geben Sie im folgenden Fenster **Adressenmaske (URL)** eine Adresse (oder eine Maske) an.

HEURISTISCHE ANALYSE VERWENDEN

Die heuristische Methode besteht in der Analyse der Aktivität, die ein Objekt im System zeigt. Wenn diese Aktivität als typisch für schädliche Objekte gilt, lässt sich ein Objekt mit hoher Wahrscheinlichkeit als schädlich oder verdächtig einstufen. Dadurch können neue Bedrohungen bereits erkannt werden, bevor die Virenanalytiker von ihrer Aktivität wissen. In der Grundeinstellung ist die heuristische Analyse aktiviert.

Kaspersky Internet Security informiert Sie darüber, wenn in einer Nachricht ein schädliches Objekt gefunden wird. Die Meldung erfordert die Auswahl einer Aktion.

Zusätzlich kann die Genauigkeitsstufe der Untersuchung festlegt werden: **oberflächlich**, **mittel** oder **tief**. Bewegen Sie dazu den Schieberegler auf die gewünschte Position.

Gehen Sie folgendermaßen vor, um die heuristische Analyse zu verwenden / zu deaktivieren und die Genauigkeitsstufe der Untersuchung festzulegen:

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.

2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Web-Anti-Virus** aus.

3. Klicken Sie für die ausgewählte Komponente auf die Schaltfläche **Einstellungen**.

4. Aktivieren / deaktivieren Sie im folgenden Fenster **Web-Anti-Virus** im Block **Untersuchungsmethoden** das Kontrollkästchen **Heuristische Analyse** und stellen Sie darunter das Genauigkeitsniveau der Untersuchung ein.

UNTERSUCHUNG OPTIMIEREN

Um die Erkennungsgenauigkeit für schädlichen Code durch Web-Anti-Virus zu steigern, wird für Objekte, die aus dem Internet eintreffen, die Zwischenspeicherung von Fragmenten verwendet. Bei Verwendung dieser Methode erfolgt die Untersuchung eines Objekts durch Web-Anti-Virus erst, nachdem es vollständig empfangen wurde. Anschließend wird

das Objekt auf Viren analysiert und entsprechend der Analyseergebnisse dem Benutzer zur Arbeit übergeben oder blockiert.

Allerdings erhöht die Verwendung dieses Algorithmus die Zeit für die Objektuntersuchung und für dessen Freigabe an den Benutzer. Außerdem können beim Kopieren und bei der Bearbeitung großer Objekte Probleme auftreten, die mit einer Zeitüberschreitung bei der Verbindung mit dem HTTP-Client zusammenhängen.

Um dieses Problem zu lösen, empfehlen wir, die Zeit für die Zwischenspeicherung von Fragmenten eines aus dem Internet empfangenden Objekts zu beschränken. Bei einer Überschreitung der festgelegten Dauer wird jeder heruntergeladene Teil der Dateien ungeprüft dem Benutzer übergeben. Nach dem Abschluss des Downloads wird das Objekt vollständig untersucht. Dadurch lässt sich die Übertragungsdauer des Objekts an den Benutzer verkürzen und das Problem einer Verbindungstrennung lösen, wobei das Sicherheitsniveau bei der Arbeit im Internet nicht gesenkt wird.

Außerdem beträgt das Zeitlimit für die Zwischenspeicherung von Dateifragmenten 1 Sekunde. Wird dieser Wert erhöht oder die Zeitbeschränkung für die Zwischenspeicherung ganz aufgehoben, so wird das Niveau der Antiviren-Untersuchung gesteigert, wobei es aber gleichzeitig zu einer gewissen Verzögerung beim Objektzugriff kommt.

Gehen Sie folgendermaßen vor, um ein Zeitlimit für die Zwischenspeicherung von Fragmenten festzulegen oder diese Beschränkung aufzuheben:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Web-Anti-Virus** aus.
3. Klicken Sie für die ausgewählte Komponente auf die Schaltfläche **Einstellungen**.
4. Aktivieren / deaktivieren Sie im folgenden Fenster **Web-Anti-Virus** im Block **Untersuchung optimieren** das Kontrollkästchen **Zwischenspeicherung von Fragmenten maximal** und geben Sie rechts im Feld den Zeitraum (in Sekunden) an.

STANDARDPARAMETER FÜR DEN WEB-SCHUTZ WIEDERHERSTELLEN

Während Sie die Arbeit von Web-Anti-Virus anpassen, können Sie jederzeit zu den empfohlenen Einstellungen zurückkehren. Diese gelten als optimal, werden von den Kaspersky-Lab-Spezialisten empfohlen und sind in der Sicherheitsstufe **Empfohlen** zusammengefasst.

Gehen Sie folgendermaßen vor, um die standardmäßigen Parameter für Web-Anti-Virus wiederherzustellen:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Web-Anti-Virus** aus.
3. Klicken Sie für die ausgewählte Komponente im Block **Sicherheitsstufe** auf die Schaltfläche **Standard**.

SCHUTZ FÜR DEN DATENVERKEHR VON INSTANT-MESSENGERN

In letzter Zeit gewinnen *Instant-Messenger*, die dem Austausch von Sofortnachrichten dienen, immer größere Popularität. Allerdings bringen sie neben nützlichen Funktionen für die Arbeit im Internet auch eine potentielle Bedrohung für die Computersicherheit mit sich. Mit Hilfe von Instant-Messengern können auch Nachrichten übertragen werden, die Links auf Seiten enthalten, die verdächtig sind oder die von Angreifern für Phishing-Angriffe verwendet werden. Schädliche Programme verwenden Instant-Messenger zum Senden von Spam-Nachrichten. Außerdem können Sofortnachrichten Links zu Programmen (oder sogar Programme) enthalten, die Nummern und Kennwörter der Benutzer stehlen.

Die Komponente *IM-Anti-Virus* dient dazu, die Sicherheit der Arbeit mit Instant-Messengern zu gewährleisten. Sie schützt die Informationen, die über Instant-Messenger-Protokolle auf Ihren Computer gelangen.

Das Produkt gewährleistet Sicherheit bei der Arbeit mit einer Vielzahl von Programmen, die dem Sofortaustausch von Nachrichten dienen. Dazu zählen ICQ, MSN, AIM, Yahoo! Messenger, Jabber, Google Talk und andere.

Die Programme Yahoo! Messenger und Google Talk arbeiten mit dem SSL-Protokoll. Damit IM-Anti-Virus den Datenverkehr dieser Programme untersucht, ist es erforderlich, die Untersuchung geschützter Verbindungen zu verwenden (s. S. 179). Aktivieren Sie dazu im Abschnitt **Netzwerk** das Kontrollkästchen **Geschützte Verbindungen untersuchen**.

Die Untersuchung des Datenverkehrs erfolgt mit einer bestimmten Auswahl von Parametern. Wenn IM-Anti-Virus in einer Nachricht eine Bedrohung findet, wird die Nachricht durch eine Warnung für den Benutzer ersetzt.

Das Schutzniveau, das auf Ihrem Computer für den Datenverkehr von Instant-Messengern gilt, wird durch eine Auswahl von Parametern festgelegt. Sie lassen sich in folgende Gruppen aufteilen:

- Parameter, die den Schutzbereich festlegen.
- Parameter, die die Untersuchungsmethoden festlegen.

Gehen Sie folgendermaßen vor, um die Funktionsparameter von IM-Anti-Virus anzupassen:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link im oberen Bereich des Fensters auf den Link **Einstellungen**.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **IM-Anti-Virus** aus.
3. Passen Sie die Parameter der ausgewählten Komponente entsprechend an.

IN DIESEM ABSCHNITT

Algorithmus für die Arbeit der Komponente 72

Schutzbereich festlegen 72

Untersuchungsmethode auswählen 72

Heuristische Analyse verwenden 73

ALGORITHMUS FÜR DIE ARBEIT DER KOMPONENTE

IM-Anti-Virus ist eine Komponente von Kaspersky Internet Security, die die Untersuchung von Nachrichten, die mit Instant-Messengern übertragen werden, auf gefährliche Objekte gewährleistet. Die Komponente wird beim Hochfahren des Betriebssystems gestartet, befindet sich ständig im Arbeitsspeicher des Computers und untersucht alle eingehenden und ausgehenden Nachrichten.

Der Datenverkehr von Instant-Messengern erfolgt standardmäßig nach folgendem Algorithmus:

1. Jede Nachricht, die vom Benutzer empfangen oder gesendet wird, wird von der Komponente abgefangen.

2. IM-Anti-Virus prüft, ob Sofortnachrichten gefährliche Objekte oder Links enthalten, die in den Datenbanken für verdächtige Webadressen und/oder Phishing-Webadressen verzeichnet sind. Wenn eine Bedrohung gefunden wird, wird der Nachrichtentext durch eine Warnung für den Benutzer ersetzt.

3. Wenn in der Nachricht kein Sicherheitsrisiko gefunden wird, erhält der Benutzer Zugriff darauf.

Die von Instant-Messenger übertragenen Dateien untersucht die Komponente Datei-Anti-Virus (s. Abschnitt "Schutz für das Dateisystems des Computers" auf S. 47) beim Speicherversuch.

SCHUTZBEREICH FESTLEGEN

Unter Schutzbereich wird der Typ der Nachrichten verstanden, die untersucht werden sollen.

- **Eingehende und ausgehende Nachrichten**. Standardmäßig untersucht der IM-Anti-Virus ein- und ausgehende Nachrichten.

- **Nur eingehende Nachrichten**. Wählen Sie diesen Parameter, wenn Sie sicher sind, dass die von Ihnen gesendeten Nachrichten keine gefährlichen Objekte enthalten. IM-Anti-Virus untersucht nur eingehende Nachrichten.

Kaspersky Internet Security untersucht standardmäßig ein- und ausgehende Nachrichten von Instant-Messengern.

Wenn Sie sicher sind, dass die von Ihnen gesendeten Nachrichten keine gefährlichen Objekte enthalten, können Sie die Untersuchung des ausgehenden Datenverkehrs deaktivieren.

Gehen Sie folgendermaßen vor, um die Untersuchung ausgehender Nachrichten zu deaktivieren:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link im oberen Bereich des Fensters auf den Link **Einstellungen**.

2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **IM-Anti-Virus** aus.

3. Wählen Sie für die ausgewählte Komponente im Block **Schutzbereich** die Variante **Nur eingehende Nachrichten**.

UNTERSUCHUNGSMETHODE AUSWÄHLEN

Die Untersuchungsmethoden beziehen sich hier auf die Untersuchung der in Instant-Messenger-Nachrichten enthaltenen Links auf ihre Zugehörigkeit zur Liste für verdächtige Adressen und / oder zur Liste der Phishing-Adressen.

- **Links mit der Datenbank für verdächtige Webadressen untersuchen**. IM-Anti-Virus prüft, ob die in den Nachrichten enthaltenen Links sich auf der schwarzen Liste befinden.

- **Links mit der Datenbank für Phishing-Webadressen untersuchen**. Die Datenbanken von Kaspersky Internet Security enthalten Informationen über die gegenwärtig bekannten Seiten, die für Phishing-Angriffe

benutzt werden. Die Datenbanken werden von den Kaspersky-Lab-Spezialisten durch Adressen erweitert, die von der internationalen Organisation zum Kampf gegen Phishing (The Anti-Phishing Working Group) zur Verfügung gestellt werden. Diese Liste wird beim Update der Datenbanken von Kaspersky Internet Security aktualisiert.

- *Gehen Sie folgendermaßen vor, um die in E-Mails enthaltenen Links mit der Datenbank für verdächtige Adressen zu untersuchen:*

  1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.

  2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **IM-Anti-Virus** aus.

  3. Aktivieren Sie für die ausgewählte Komponente im Block **Untersuchungsmethoden** das Kontrollkästchen **Links mit Datenbank für verdächtige Webadressen untersuchen**.

- *Gehen Sie folgendermaßen vor, um die in E-Mails enthaltenen Links mit der Datenbank für verdächtige Adressen zu untersuchen:*

  1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link im oberen Bereich des Fensters auf den Link **Einstellungen**.

  2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **IM-Anti-Virus** aus.

  3. Aktivieren Sie für die ausgewählte Komponente im Block **Untersuchungsmethoden** das Kontrollkästchen **Links mit Datenbank für Phishing-Webadressen untersuchen**.

HEURISTISCHE ANALYSE VERWENDEN

Die heuristische Methode besteht in der Analyse der Aktivität, die ein Objekt im System zeigt. Zu diesem Zweck werden alle Skripts, die in Instant-Messenger-Nachrichten enthalten sind, in einer geschützten Umgebung ausgeführt. Wenn die erkannte Aktivität eines Skripts als typisch für schädliche Objekte gilt, lässt sich das Objekt mit hoher Wahrscheinlichkeit als schädlich oder verdächtig einstufen. In der Grundeinstellung ist die heuristische Analyse aktiviert.

Kaspersky Internet Security informiert Sie darüber, wenn in einer Nachricht ein schädliches Objekt gefunden wird.

Zusätzlich können Sie das Genauigkeitsniveau der Untersuchung festlegen: **oberflächlich**, **mittel** oder **tief**. Bewegen Sie dazu den Schieberegler auf die gewünschte Position.

- *Gehen Sie folgendermaßen vor, um die heuristische Analyse zu verwenden / zu deaktivieren und die Genauigkeitsstufe der Untersuchung festzulegen:*

  1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link im oberen Bereich des Fensters auf den Link **Einstellungen**.

  2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **IM-Anti-Virus** aus.

  3. Aktivieren / deaktivieren Sie für die ausgewählte Komponente im Block **Untersuchungsmethoden** das Kontrollkästchen **Heuristische Analyse** stellen Sie darunter das Genauigkeitsniveau ein.

PROGRAMMKONTROLLE

Hinsichtlich der Systemsicherheit lassen sich alle Programme in drei Gruppen unterteilen:

- *Sichere*. Zu dieser Gruppe gehören Programme, die von bekannten Herstellern stammen und digitale Signaturen besitzen. Solchen Programmen kann erlaubt werden, beliebige Aktionen im System auszuführen.
- *Gefährliche*. Unter diese Gruppe fallen die momentan bekannten Bedrohungen. Die Aktivität von Programmen dieser Gruppe muss blockiert werden.
- *Unbekannte*. Zu dieser Gruppe lassen sich Programme zählen, die nicht von bekannten Herstellern stammen und keine digitale Signatur besitzen. Sie fügen dem System nicht unbedingt Schaden zu, aber eine eindeutige Entscheidung über die Sicherheit der Verwendung von Programmen dieser Gruppe kann erst nach einer Verhaltensanalyse getroffen werden. Bevor eine Entscheidung über die Sicherheit eines unbekannten Programms getroffen wird, ist es vernünftig, den Zugriff auf die Systemressourcen einzuschränken.

Die Komponente Programmkontrolle registriert die Aktionen, die von Programmen im System ausgeführt werden können, und reguliert in Abhängigkeit von der Gruppe, zu der die Programme gehören (s. Abschnitt "Programmgruppen" auf S. 76), ihre Aktivität. Für jede Gruppe von Programmen ist eine Auswahl von Regeln (s. Abschnitt "Regeln für die Programmkontrolle" auf S. 79) vorgegeben. Diese Regeln steuern den Zugriff von Programmen auf unterschiedliche Ressourcen:

- Dateien und Ordner
- Registrierungsschlüssel
- Netzwerkadressen
- Ausführungsumgebung

Beim Zugriff eines Programms auf eine Ressource untersucht die Komponente, ob das Programm die erforderlichen Zugriffsrechte besitzt, und führt die von einer Regel vorgegebene Aktion aus.

Gehen Sie folgendermaßen vor, um die Programmkontrolle anzupassen:

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Programmkontrolle** aus.
3. Passen Sie die Parameter der ausgewählten Komponente entsprechend an.

und:

1. Öffnen Sie das Programmhauptfenster und wählen Sie den Abschnitt Programmkontrolle aus.
2. Klicken Sie auf der rechten Seite des Fensters auf den Link **Programmaktivität**.
3. Nehmen Sie im folgenden Fenster **Aktivitätskontrolle für Programme** die erforderlichen Änderungen vor.

IN DIESEM ABSCHNITT

Algorithmus für die Arbeit der Komponente 75

Schutzbereich festlegen 77

Regeln für die Programmkontrolle 79

ALGORITHMUS FÜR DIE ARBEIT DER KOMPONENTE

Wenn ein Programm zum ersten Mal gestartet wird, wird es nach folgendem Algorithmus von der Programmkontrolle überprüft:

1. Das Programm wird auf Viren untersucht.

2. Es wird geprüft, ob das Programm eine digitale Signatur besitzt. Wenn eine digitale Signatur vorhanden ist, wird das Programm der Gruppe **Vertrauenswürdig** zugeordnet. Wenn das Programm keine digitale Signatur besitzt (oder die digitale Signatur beschädigt ist oder auf der schwarzen Liste steht), führt die Komponente den nächsten Schritt aus.

3. Es wird geprüft, ob die interne Datenbank für bekannte Software einen Eintrag über das zu startende Programm enthält. Diese Datenbank gehört zum Lieferumfang von Kaspersky Internet Security. Wenn die Datenbank einen Eintrag enthält, der sich auf das zu startende Programm bezieht, wird es der entsprechenden Gruppe zugeordnet. Wenn in der Datenbank kein Eintrag über das Programm gefunden wird, führt die Komponente den nächsten Schritt aus.

4. Es werden Informationen über die ausführbare Programmdatei an die Datenbank für bekannte Software gesendet, die sich auf einem Kaspersky-Lab-Server befindet. Wenn die Datenbank einen Eintrag enthält, der den gesendeten Informationen entspricht, wird das Programm der entsprechenden Gruppe zugeordnet. Wenn keinen Verbindung mit der Datenbank möglich ist (wenn beispielsweise keine Internetverbindung besteht), führt die Komponente den nächsten Schritt aus.

5. Es wird mit Hilfe der heuristischen Analyse eine Risikobewertung des Programms vorgenommen. Programme mit einem niedrigen Risikowert werden der Gruppe **Schwach beschränkt** zugeordnet. Wenn sich ein hoher Risikowert ergibt, werden Sie von Kaspersky Internet Security darüber informiert und Sie können eine Gruppe auswählen, der das Programm zugeordnet werden soll.

Nachdem alle Untersuchungen abgeschlossen wurden, erscheint auf dem Bildschirm eine Meldung über die Entscheidung, die für dieses Programm getroffen wurde. Für Programme, die der Gruppe **Vertrauenswürdig** zugeordnet werden, ist die Meldung in der Grundeinstellung deaktiviert.

Beim wiederholten Start eines Programms kontrolliert die Programmkontrolle seine Integrität. Wenn ein Programm nicht verändert wurde, wendet die Komponente die bestehende Regel darauf an. Wenn ein Programm verändert wurde, überprüft die Programmkontrolle es nach dem oben beschriebenen Algorithmus.

SIEHE AUCH

Rechte erben 75

Risikobewertung 76

Programmgruppen 76

Startfolge eines Programms. 77

RECHTE ERBEN

Der Mechanismus zum *Erben von Rechten* ist ein wichtiger Bestandteil der Komponente Programmkontrolle. Dieser Mechanismus verhindert, dass vertrauenswürdige Programme von zweifelhaften Programmen oder von Programmen, die über beschränkte Rechte verfügen, dazu benutzt werden, privilegierte Aktionen auszuführen.

Wenn ein Programm versucht, Zugriff auf eine kontrollierte Ressource zu erhalten, analysiert die Programmkontrolle für alle übergeordneten Programmprozesse die Rechte für den Zugriff auf die Ressource. Dabei wird die *Regel mit der minimalen Priorität* ausgeführt: Beim Vergleich von Zugriffsrechten eines Programms und eines übergeordneten Prozesses werden auf die Programmaktivität die Zugriffsrechte mit der geringsten Priorität angewendet.

Priorität der Zugriffsrechte:

1. **Erlauben**. Diese Zugriffsrechte besitzen die höchste Priorität.

2. **Benutzer fragen**.

3. **Blockieren**. Diese Zugriffsrechte besitzen die niedrigste Priorität.

Beispiel:

Ein trojanisches Programm versucht, das Programm *regedit.exe* zu verwenden, um die Registrierung von Microsoft Windows zu manipulieren. In der Regel für ein trojanisches Programm ist als Reaktion für den Zugriff auf die Registrierung die Aktion **Blockieren**, festgelegt, in der Regel für *regedit.exe* die Aktion **Erlauben**.

Folglich wird die Aktivität von *regedit.exe*, das von einem trojanischen Programm gestartet wurde, blockiert, weil *regedit.exe* seine Rechte von dem übergeordneten Prozess erbt. Dabei wird die Regel der minimalen Priorität ausgelöst – die Aktion wird unabhängig davon blockiert, ob für das Programm *regedit.exe* Erlaubnisregeln vorhanden sind.

Wenn die Aktivität eines Programms blockiert wird, weil ein übergeordneter Prozess unzureichende Rechte besitzt, können Sie diese Rechte anpassen (s. Abschnitt "Regel für ein Programm ändern" auf S. 81).

Das Ändern von Rechten eines übergeordneten Prozesses oder das Ausschalten des Vererbungsmechanismus sollte nur dann erfolgen, wenn Sie absolut sicher sind, dass die Aktivität des Prozesses keine Gefahr für das System darstellt!

SIEHE AUCH

Startfolge eines Programms. 77

RISIKOBEWERTUNG

Für jedes Programm, das auf Ihrem Computer gestartet werden soll, ermittelt die Programmkontrolle mit Hilfe der heuristischen Analyse einen Risikowert. Der *Risikowert* ist eine Kennziffer für die Gefährlichkeit, die ein Programm für das System darstellt, und beruht auf zwei Typen von Kriterien:

- Zu diesen Kriterien gehören Informationen über die ausführbare Datei des Programms: Dateigröße, Erstellungsdatum usw.

- Diese Kriterien werden verwendet, um die Arbeit des Programms in einer virtuellen Umgebung zu modellieren (Analyse der Aufrufe von Systemfunktionen durch das Programm). Die Analyse solcher Kriterien erlaubt es, für Schadprogramme typisches Verhalten zu erkennen.

In Übereinstimmung mit den ermittelten Werten werden die Programme von der Programmkontrolle bestimmten Gruppen (s. Abschnitt "Programmgruppen" auf S. 76) zugeordnet. Je niedriger die Risikobewertung, desto mehr Aktionen werden einem Programm im System erlaubt.

PROGRAMMGRUPPEN

Alle auf dem Computer gestarteten Programme werden von der Programmkontrolle in Gruppen eingeordnet. Als Kriterien gelten die Gefährlichkeit für das System und die Zugriffsrechte von Programmen auf Systemressourcen.

Es gibt vier vordefinierte Gruppen von Programmen:

- **Vertrauenswürdig**. Programme, die über die digitale Signatur eines vertrauenswürdigen Herstellers verfügen und die in der Datenbank für vertrauenswürdige Programme enthalten sind. Für solche Programme bestehen keine Beschränkungen für im System ausführbare Aktionen. Die Aktivität dieser Programme wird vom Proaktiven Schutz und von Datei-Anti-Virus kontrolliert.

- **Schwach beschränkt**. Programme, die keine digitale Signatur eines vertrauenswürdigen Herstellers besitzen oder nicht in der Datenbank für bekannte Programme enthalten sind. Diese Programme besitzen allerdings einen niedrigen Risikowert (auf S. 76). Ihnen werden bestimmte Operationen erlaubt, z.B. Zugriff auf andere Prozesse, Systemsteuerung, versteckter Zugriff auf ein Netzwerk. Für die Mehrzahl der Operationen ist eine Erlaubnis des Benutzers erforderlich.

- **Stark beschränkt**. Programme, die keine digitale Signatur besitzen oder nicht in der Datenbank für vertrauenswürdige Programme enthalten sind. Diese Programme besitzen einen hohen Risikowert. Für die Mehrzahl der Aktionen, die von Programmen dieser Gruppe im System ausgeführt werden sollen, ist eine Erlaubnis des Benutzers erforderlich.

- **Nicht vertrauenswürdig**. Programme, die keine digitale Signatur besitzen oder nicht in der Datenbank für vertrauenswürdige Programme enthalten sind. Diese Programme besitzen einen sehr hohen Risikowert. Die Programmkontrolle sperrt alle Aktionen dieser Programme.

Programme, die von der Programmkontrolle einer bestimmten Gruppe zugeordnet werden, erhalten einen entsprechenden Status und erben die Rechte für den Zugriff auf Ressourcen von der Regel (s. Abschnitt "Regeln für die Programmkontrolle" auf S. 79) der Gruppe.

Die Spezialisten von Kaspersky Lab warnen davor, Programme in andere Gruppen zu verschieben. Stattdessen können bei Bedarf die Zugriffsrechte eines Programms auf konkrete Systemressourcen geändert werden (s. Abschnitt "Regel für ein Programm ändern" auf S. 81).

STARTFOLGE EINES PROGRAMMS.

Als Initiator für den Start eines Programms kann entweder der Benutzer oder ein anderes laufendes Programm auftreten.

Wenn ein anderes Programm als Initiator auftritt, entsteht eine Startfolge, die übergeordnete und untergeordnete Programme umfasst. Die Startfolge kann gespeichert werden.

Beim Speichern einer Startfolge verbleibt jedes Programm, das zu dieser Startfolge gehört, in seiner Gruppe.

SIEHE AUCH

Rechte erben 75

SCHUTZBEREICH FESTLEGEN

Die Programmkontrolle verwaltet die Rechte von Programmen, die für das Ausführen von Aktionen mit folgenden Ressourcenkategorien gelten:

Betriebssystem. Zu dieser Kategorie gehören:

- Registrierungsschlüssel, die Parameter für den automatischen Start enthalten.
- Registrierungsschlüssel, die Parameter für die Arbeit im Internet enthalten.
- Registrierungsschlüssel, die die Systemsicherheit beeinflussen.
- Registrierungsschlüssel, die Parameter für Systemdienste enthalten.
- Systemdateien und Systemordner
- Autostart-Ordner

Die Spezialisten von Kaspersky Lab haben eine Liste mit Kategorien der Parameter und Ressourcen des Betriebssystems erstellt, die immer von Kaspersky Internet Security geschützt werden. Diese Liste kann nicht verändert werden. Allerdings können Sie die Kontrolle bestimmter Objekte des Betriebssystems in der ausgewählten Kategorie deaktivieren sowie diese Liste erweitern.

Persönliche Daten. Zu dieser Kategorie gehören:

- Dateien des Benutzers (Ordner Eigene Dateien (My Documents), Cookies-Dateien, Daten über Benutzeraktivität).
- Dateien, Ordner und Registrierungsschlüssel, die Funktionsparameter und wichtige Daten für häufig verwendete Programme enthalten: Internetbrowser, Dateimanager, Mailprogramme, Instant-Messenger und elektronische Zahlungssysteme.

Die Spezialisten von Kaspersky Lab haben eine Liste mit Kategorien der Ressourcen erstellt, die immer von Kaspersky Internet Security geschützt werden. Diese Liste kann nicht verändert werden. Allerdings können Sie die Kontrolle einer bestimmten Ressourcenkategorie deaktivieren sowie diese Liste erweitern.

Gehen Sie folgendermaßen vor, um die Liste der zu schützenden persönlichen Daten zu erweitern:

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Programmkontrolle** aus.
3. Klicken Sie für die ausgewählte Komponente auf die Schaltfläche **Einstellungen**.
4. Wählen Sie im folgenden Fenster auf der Registerkarte **Persönliche Daten** in der Dropdown-Liste **Kategorie** die erforderliche Objektkategorie für persönliche Daten aus und klicken Sie auf den Link **Hinzufügen** (klicken Sie auf den Link **Kategorie hinzufügen**, wenn eine neue Kategorie von zu schützenden Ressourcen hinzugefügt werden soll, und geben Sie im folgenden Fenster ihren Namen ein).
5. Wählen Sie im Kontextmenü den erforderlichen Ressourcentyp aus:
   - **Datei oder Ordner**. Geben Sie im folgenden Fenster **Datei oder Ordner auswählen** eine Datei oder einen Ordner an.
   - **Registrierungsschlüssel**. Geben Sie im folgenden Fenster **Registrierungsobjekt auswählen** den zu schützenden Registrierungsschlüssel an.
   - **Netzwerkdienst**. Geben Sie im folgenden Fenster **Netzwerkdienst** die Parameter der zu kontrollierenden Netzwerkverbindung an (s. Abschnitt "Parameter eines Netzwerkdiensts anpassen" auf S. 95).
   - **IP-Adresse(n)**. Geben Sie im folgenden Fenster **Netzwerkadressen** den zu schützenden Adressenbereich an.

   Nachdem eine Ressource dem Schutzbereich hinzugefügt wurde, kann sie geändert oder gelöscht werden. Dazu dienen die entsprechenden Links im unteren Bereich der Registerkarte. Wenn Sie eine Ressource aus dem Schutzbereich ausschließen möchten, deaktivieren Sie das entsprechende Kontrollkästchen ☑.

Gehen Sie folgendermaßen vor, um die Liste der zu schützenden Parameter und Ressourcen des Betriebssystems zu erweitern:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Programmkontrolle** aus.
3. Klicken Sie für die ausgewählte Komponente auf die Schaltfläche **Einstellungen**.

4. Wählen Sie im folgenden Fenster auf der Registerkarte **Betriebssystem** in der Dropdown-Liste **Kategorie** die erforderliche Kategorie für Objekte des Betriebssystems aus und klicken Sie auf den Link **Hinzufügen**.

5. Wählen Sie in Abhängigkeit von der ausgewählten Kategorie den erforderlichen Ressourcentyp aus:

   - **Datei oder Ordner**. Geben Sie im folgenden Fenster **Datei oder Ordner auswählen** eine Datei oder einen Ordner an.

   - **Registrierungsschlüssel**. Geben Sie im folgenden Fenster **Registrierungsobjekt auswählen** den zu schützenden Registrierungsschlüssel an.

   Nachdem eine Ressource dem Schutzbereich hinzugefügt wurde, kann sie geändert oder gelöscht werden. Dazu dienen die entsprechenden Links im unteren Bereich der Registerkarte. Wenn Sie eine Ressource aus dem Schutzbereich ausschließen möchten, deaktivieren Sie das entsprechende Kontrollkästchen .

REGELN FÜR DIE PROGRAMMKONTROLLE

Regel – Kombination von Reaktionen der Programmkontrolle für kontrollierte Ressourcen (s. Abschnitt "Schutzbereich festlegen" auf S. 77).

Mögliche Reaktionen der Komponente:

- **Erben**. Die Programmkontrolle wendet auf die Aktivität des Programms jene Regel an, die für die Gruppe, zu der das Programm gehört, festgelegt wurde. Diese Reaktion wird standardmäßig angewendet.

- **Erlauben**. Die Programmkontrolle erlaubt dem Programm, die Aktion auszuführen.

- **Verbieten**. Die Programmkontrolle erlaubt dem Programm nicht, die Aktion auszuführen.

- **Aktion erfragen**. Die Programmkontrolle informiert den Benutzer darüber, dass das Programm versucht, die Aktion auszuführen, und fragt den Benutzer nach dem weiteren Vorgehen.

- **Protokollieren**. Informationen über die Aktivität des Programms und die Reaktion der Programmkontrolle werden im Bericht aufgezeichnet. Die Option zum Protokollieren kann in Verbindung mit jeder anderen Aktion der Komponente verwendet werden.

Ein Programm erbt standardmäßig die Zugriffsrechte der Gruppe, zu der es gehört. Sie können eine Regel für ein Programm ändern. In diesem Fall besitzen die Regeln für das Programm eine höhere Priorität als die Regeln für die Gruppe, der das Programm angehört.

SIEHE AUCH

Programme zu Gruppen zuordnen 80

Dauer der Statusermittlung für ein Programm ändern 80

Regel für ein Programm ändern 81

Regel für eine Programmgruppe ändern 81

Netzwerkregel für ein Programm erstellen 82

Ausnahmen anpassen 82

Regeln für Programme löschen 83

PROGRAMME ZU GRUPPEN ZUORDNEN

Programme, die von der Komponente Programmkontrolle der Gruppe (s. Abschnitt "Programmgruppen" auf S. 76) **Vertrauenswürdig** zugeordnet werden, stellen keine Gefahr für das System dar.

Es besteht die Möglichkeit, eine Liste mit vertrauenswürdigen Programmen anzulegen, deren Aktivität nicht von der Programmkontrolle überwacht werden soll. Programme, die eine digitale Signatur besitzen oder in der Datenbank von Kaspersky Security Network enthalten sind, können als vertrauenswürdig eingestuft werden.

Für andere Programme, die nicht zur vertrauenswürdigen Gruppe gehören, können Sie entweder die heuristische Analyse verwenden, um die entsprechende Gruppe zu ermitteln, oder die Gruppe festlegen, der ein Programm automatisch zugeordnet werden soll.

- *Gehen Sie folgendermaßen vor, damit die Programmkontrolle Programme, die eine digitale Signatur besitzen und / oder in der Datenbank von Kaspersky Security Network enthalten sind, als vertrauenswürdig betrachtet und nicht über ihre Aktivität informiert:*

  1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
  2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Programmkontrolle** aus.
  3. Aktivieren Sie für die ausgewählte Komponente im Block **Vertrauenswürdige Programme** das Kontrollkästchen ☑ **Mit digitaler Signatur** und / oder das Kontrollkästchen ☑ **Die in der Datenbank von Kaspersky Security Network enthalten sind**.

- *Gehen Sie folgendermaßen vor, damit die Programmkontrolle die heuristische Analyse verwendet, um nicht vertrauenswürdige Programme den entsprechenden Gruppen zuzuordnen:*

  1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
  2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Programmkontrolle** aus.
  3. Wählen Sie für die ausgewählte Komponente im Block **Vertrauenswürdige Programme** die Variante ◉ **Zur Statusermittlung die heuristische Analyse verwenden** aus. Ein Programm wird der Gruppe zugeordnet, die dem ermittelten Status entspricht.

- *Gehen Sie folgendermaßen vor, damit die Programmkontrolle automatisch einen festgelegten Status zuweist, um nicht vertrauenswürdige Programme den entsprechenden Gruppen zuzuordnen:*

  1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
  2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Programmkontrolle** aus.
  3. Wählen Sie für die ausgewählte Komponente im Block **Vertrauenswürdige Programme** die Variante ◉ **Status automatisch zuweisen** aus und wählen Sie den erforderlichen Status aus der Dropdown-Liste auf der rechten Seite aus. Programme werden der Gruppe zugeordnet, die dem ermittelten Status entspricht.

DAUER DER STATUSERMITTLUNG FÜR EIN PROGRAMM ÄNDERN

Wenn die Statusermittlung für ein Programm mit der heuristischen Analyse erfolgt, wird ein Programm von der Programmkontrolle standardmäßig für 30 Sekunden untersucht. Wenn die Risikobewertung innerhalb dieses Zeitraums nicht abgeschlossen wurde, erhält das Programm den Status *Schwach beschränkt* und wird der entsprechenden Gruppe zugewiesen.

Die Risikobewertung wird im Hintergrundmodus fortgesetzt. Nachdem die heuristische Analyse des Programms abgeschlossen ist, erhält es den seinem Risikowert entsprechenden Status und wird in die entsprechende Gruppe verschoben.

Sie können die Dauer ändern, für die gestartete Programme von der Komponente analysiert werden sollen. Wenn Sie sicher sind, dass alle Programme, die auf Ihrem Computer gestartet werden, kein Sicherheitsrisiko darstellen, können Sie die für die Analyse vorgesehene Dauer verringern. Sollten Sie hingegen Software auf dem Computer installieren, an deren Sicherheit Sie zweifeln, so wird empfohlen, die Analysedauer zu erhöhen.

Gehen Sie folgendermaßen vor, um die Dauer, die für die Analyse unbekannter Programme vorgesehen ist, zu ändern:

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Programmkontrolle** aus.
3. Aktivieren Sie für die ausgewählte Komponente im Block **Erweitert** den Parameterwert **Maximale Dauer für Statusermittlung eines Programms**.

REGEL FÜR EIN PROGRAMM ÄNDERN

Wenn ein Programm zum ersten Mal gestartet wird, ermittelt die Programmkontrolle seinen Status und weist es der entsprechenden Gruppe zu. Dann registriert die Komponente die Aktionen, die von diesem Programm im System ausgeführt werden können, und reguliert in Abhängigkeit von der Gruppe zu der es gehört, (s. Abschnitt "Programmgruppen" auf S. 76) seine Aktivität. Beim Zugriff eines Programms auf eine Ressource untersucht die Komponente, ob das Programm die erforderlichen Zugriffsrechte besitzt, und führt die von einer Regel vorgegebene Aktion aus. Sie können eine Regel die erstellt wurde ändern, wenn der Status für das Programm ermittelt und es in die entsprechende Gruppe verschoben wurde.

Gehen Sie folgendermaßen vor, um eine Regel für ein Programm zu ändern:

1. Öffnen Sie das Programmhauptfenster und wählen Sie den Abschnitt **Programmkontrolle** aus.
2. Klicken Sie im folgenden Fenster im Block **Programmkontrolle** auf den Link **Programmaktivität**.
3. Wählen Sie im folgenden Fenster **Aktivitätskontrolle für Programme** in der Dropdown-Liste **Kategorie** die entsprechende Kategorie aus.
4. Führen Sie für das erforderliche Programm in der Spalte **Status** einen Linksklick auf den Link mit dem Programmstatus aus.
5. Wählen Sie im Kontextmenü den Punkt **Benutzerdefinierte Parameter** aus.
6. Ändern Sie im folgenden Fenster auf der Registerkarte **Regeln** die Zugriffsrechte für die entsprechende Ressourcenkategorie.

REGEL FÜR EINE PROGRAMMGRUPPE ÄNDERN

Wenn ein Programm zum ersten Mal gestartet wird, ermittelt die Programmkontrolle seinen Status und weist es der entsprechenden Gruppe zu. Dann registriert die Komponente die Aktionen, die von diesem Programm im System ausgeführt werden können, und reguliert in Abhängigkeit von der Gruppe, zu der es gehört (s. Abschnitt "Programmgruppen" auf S. 76) seine Aktivität. Bei Bedarf können Sie eine Regel für eine Gruppe ändern.

Gehen Sie folgendermaßen vor, um eine Regel für eine Gruppe zu ändern:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Programmkontrolle** aus.
3. Klicken Sie für die ausgewählte Komponente im Block **Regeln für Programmstatus** auf die Schaltfläche **Regeln anpassen**.
4. Wählen Sie im folgenden Fenster **Regeln für Aktivitätskontrolle anpassen** die entsprechende Gruppe aus.

5. Ändern Sie im folgenden Fenster auf der Registerkarte **Regeln** die Zugriffsrechte für die entsprechende Ressourcenkategorie.

NETZWERKREGEL FÜR EIN PROGRAMM ERSTELLEN

In der Grundeinstellung verschiebt die Programmkontrolle ein Programm nach seinem ersten Start in eine vordefinierte Gruppe. Eine Gruppenregel reguliert den Zugriff des Programms auf Netzwerke mit einem bestimmten Status. Wenn es erforderlich ist, den Zugriff eines Programms auf bestimmte Netzwerkdienste auf spezielle Weise zu verarbeiten, können Sie eine Netzwerkregel erstellen.

Gehen Sie folgendermaßen vor, um eine Regel zu erstellen, die die Netzwerkaktivität eines Programms reguliert:

1. Öffnen Sie das Programmhauptfenster und wählen Sie den Abschnitt **Programmkontrolle** aus.
2. Klicken Sie im folgenden Fenster im Block **Programmkontrolle** auf den Link **Programmaktivität**.
3. Wählen Sie im folgenden Fenster **Aktivitätskontrolle für Programme** in der Dropdown-Liste **Kategorie** die erforderliche Kategorie aus.
4. Führen Sie für das erforderliche Programm in der Spalte **Status** einen Linksklick auf den Link mit dem Programmstatus aus.
5. Wählen Sie im Kontextmenü den Punkt **Benutzerdefinierte Parameter** aus.
6. Wählen Sie im folgenden Fenster auf der Registerkarte **Regeln** in der Dropdown-Liste die Kategorie **Netzwerkregel** aus und klicken Sie auf den Link **Hinzufügen**.
7. Legen Sie im folgenden Fenster **Netzwerkregel** die Parameter für die Paketregel fest.
8. Legen Sie die Priorität der neuen Regel fest.

AUSNAHMEN ANPASSEN

Wenn eine Regel für ein Programm erstellt wird, kontrolliert Kaspersky Internet Security standardmäßig alle Aktionen des Programms: Zugriff auf Dateien und Ordner, Zugriff auf die Ausführungsumgebung und Zugriff auf ein Netzwerk. Sie können bestimmte Aktionen von Programmen von der Untersuchung ausschließen.

Gehen Sie folgendermaßen vor, um die Aktionen eines Programms von der Untersuchung auszuschließen:

1. Öffnen Sie das Programmhauptfenster und wählen Sie den Abschnitt **Programmkontrolle** aus.
2. Klicken Sie im folgenden Fenster im Block **Programmkontrolle** auf den Link **Programmaktivität**.
3. Wählen Sie im folgenden Fenster **Aktivitätskontrolle für Programme** in der Dropdown-Liste **Kategorie** die erforderliche Kategorie aus.
4. Führen Sie für das erforderliche Programm in der Spalte **Status** einen Linksklick auf den Link mit dem Programmstatus aus.
5. Wählen Sie im Kontextmenü den Punkt **Benutzerdefinierte Parameter** aus.
6. Aktivieren Sie im folgenden Fenster auf der Registerkarte **Ausnahmen** die Kontrollkästchen der auszuschließenden Aktionen. Wenn der Netzwerkverkehr eines Programms von der Untersuchung ausgeschlossen wird, passen Sie die zusätzlichen Parameter der Ausnahme an.

   Alle Ausnahmen, die in den Regeln für Programme erstellt wurden, stehen im Konfigurationsfenster für die Programmparameter im Abschnitt **Gefahren und Ausnahmen** zur Verfügung.

REGELN FÜR PROGRAMME LÖSCHEN

Regeln für Programme, die seit einer bestimmten Zeit nicht gestartet wurden, können automatisch gelöscht werden.

Gehen Sie folgendermaßen vor, damit Regeln für Programme, die während eines bestimmten Zeitraums nicht gestartet wurden, gelöscht werden:

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.

2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Programmkontrolle** aus.

3. Aktivieren Sie für die ausgewählte Komponente im Block **Erweitert** das Kontrollkästchen **Regeln für Programme löschen, wenn nicht gestartet seit** und geben Sie im Feld rechts die entsprechende Anzahl der Tage an.

SICHERE UMGEBUNG FÜR DIE AUSFÜHRUNG VON PROGRAMMEN

Auf Computern mit Microsoft Windows XP x64 steht die Sichere Umgebung für die Ausführung von Programmen nicht zur Verfügung.

Um maximale Sicherheit für Objekte des Betriebssystems und für persönliche Daten zu gewährleisten, besteht die Möglichkeit, Programme von Drittherstellern in einer geschützten virtuellen Umgebung zu starten. Dies ist die *Sichere Umgebung*.

In der Sicheren Umgebung sollten Programme gestartet werden, an deren Sicherheit Sie zweifeln. Dadurch lassen sich Veränderungen von Objekten des Betriebssystems verhindern, die zu Funktionsstörungen führen können.

Auf Computern mit dem Betriebssystem Microsoft Windows Vista x64 kann die Funktionalität bestimmter Programme bei der Arbeit in der Sicheren Umgebung eingeschränkt sein. Beim Start solcher Programme erscheint eine entsprechende Meldung auf dem Bildschirm, wenn die Meldungen (s. S. 182) über das Ereignis **Die Funktionalität des Programms in der Sicheren Umgebung ist eingeschränkt** aktiviert wurden.

Der Start von Internetbrowsern in der Sicheren Umgebung gewährleistet die gefahrlose Ansicht von Webressourcen und schützt den Computer dabei vor dem Eindringen schädlicher Programme und die Benutzerdaten vor unerlaubten Veränderungen oder dem Löschen. Andrerseits bietet er die Möglichkeit, alle Objekte zu löschen, die während einer Internetsitzung gesammelt wurden (temporäre Dateien, Cookies, Chronik der besuchten Webseiten usw.). Microsoft Internet Explorer gehört zur Liste der Programme, die standardmäßig in der Sicheren Umgebung gestartet werden.

Der Start eines Programms in der Sicheren Umgebung erfolgt in Übereinstimmung mit dem ausgewählten Modus. Zum schnellen Start von Programmen in der Sicheren Umgebung besteht die Möglichkeit, Verknüpfungen zu erstellen.

Damit Dateien, die in der Sicheren Umgebung gespeichert oder verändert werden, auch bei der Arbeit im normalen Modus verfügbar sind, muss der speziell dafür vorgesehene gemeinsame Ordner der Sicheren Umgebung verwendet werden. Dieser steht in der Sicheren Umgebung und im normalen Modus zur Verfügung. Dateien, die sich in diesem Ordner befinden, werden bei einer Bereinigung der Sicheren Umgebung (s. S. 88) nicht gelöscht.

Es wird empfohlen, die Programme, mit denen Sie später in der Sicheren Umgebung arbeiten möchten, in der normalen Umgebung von Microsoft Windows zu installieren.

IN DIESEM ABSCHNITT

Start eines Programms in der Sicheren Umgebung 85

Verknüpfung für den Start von Programmen erstellen 85

Liste der Programme erstellen, die in der Sicheren Umgebung gestartet werden sollen 86

Modus auswählen: Programm starten 86

Modus auswählen: Daten der Sicheren Umgebung löschen 87

Gemeinsamen Ordner verwenden 87

Sicheren Umgebung bereinigen 88

START EINES PROGRAMMS IN DER SICHEREN UMGEBUNG

Wenn für ein Programm nicht der Modus **Immer im sicheren Modus starten** festgelegt wurde, bestehen folgende Möglichkeiten, um das Programm in der Sicheren Umgebung zu starten:

- aus dem Kontextmenü von Microsoft Windows.
- aus dem Hauptfenster von Kaspersky Internet Security (s. Abschnitt "Hauptfenster von Kaspersky Internet Security" auf S. 43).
- mit Hilfe einer zuvor erstellten Verknüpfung (s. Abschnitt "Verknüpfung für den Start von Programmen erstellen" auf S. 85).

Wenn für ein Programm der Modus **Immer im sicheren Modus starten** festgelegt wurde, wird das Programm unabhängig von der Startmethode immer in der Sicheren Umgebung gestartet.

Für Programme, die in der Sicheren Umgebung gestartet wurden, besitzt das Programmfenster einen grünen Rahmen. Außerdem werden die Programme in der Liste der Programme, die von Programmkontrolle kontrolliert werden in grün hervorgehoben (s. Abschnitt "Programmkontrolle" auf S. 74).

Gehen Sie folgendermaßen vor, um ein Programm mit Hilfe einer Verknüpfung zu starten:

1. Öffnen Sie den Ordner, in dem Sie die Verknüpfung erstellt haben.
2. Starten Sie das Programm durch Doppelklick auf die Verknüpfung.

Gehen Sie folgendermaßen vor, um ein Programm in der Sicheren Umgebung aus dem Hauptfenster von Kaspersky Internet Security zu starten:

1. Öffnen Sie das Programmhauptfenster.
2. Wählen Sie auf der linken Seite des Fensters den Abschnitt **Programmkontrolle**.
3. Wählen Sie im unteren Bereich des Fensters das Symbol des gewünschten Programms aus.
4. Starten Sie die Ausführung des Programms entweder durch Doppelklick auf das entsprechende Symbol, oder öffnen Sie das Kontextmenü und verwenden Sie den Punkt **Start**.

Gehen Sie folgendermaßen vor, um ein Programm in der Sicheren Umgebung aus dem Kontextmenü von Microsoft Windows zu starten:

1. Klicken Sie mit der rechten Maustaste auf den Namen des ausgewählten Objekts: Verknüpfung oder ausführbare Programmdatei.
2. Wählen Sie im Kontextmenü den Punkt **In Sicherer Umgebung starten**.

VERKNÜPFUNG FÜR DEN START VON PROGRAMMEN ERSTELLEN

Zum schnellen Start von Programmen in der Sicheren Umgebung besteht in Kaspersky Internet Security die Möglichkeit, Verknüpfungen zu erstellen. So kann das erforderliche Programm gestartet werden, ohne das Programmhauptfenster oder das Kontextmenü von Microsoft Windows zu öffnen.

Gehen Sie folgendermaßen vor, um eine Verknüpfung für den Start eines Programms in der Sicheren Umgebung zu erstellen:

1. Öffnen Sie das Programmhauptfenster.

2. Wählen Sie auf der linken Seite des Fensters den Abschnitt **Programmkontrolle**.

3. Wählen Sie im unteren Bereich des Fensters im Feld **Programme, die in der Sicheren Umgebung gestartet werden** das Symbol des erforderlichen Programms aus.

4. Öffnen Sie durch Rechtsklick das Kontextmenü und verwenden Sie den Punkt **Verknüpfung erstellen**.

5. Geben Sie im folgenden Fenster an, wo und unter welchem Namen die Verknüpfung gespeichert werden soll. Standardmäßig wird die Verknüpfung im Ordner *Arbeitsplatz* des aktiven Computerbenutzers erstellt und erhält einen Namen, der dem Programmprozess entspricht.

LISTE DER PROGRAMME ERSTELLEN, DIE IN DER SICHEREN UMGEBUNG GESTARTET WERDEN SOLLEN

Im Programmhauptfenster kann eine Liste der Programme angelegt werden, die in der Sicheren Umgebung gestartet werden sollen. Diese Liste befindet sich im Abschnitt **Programmkontrolle**.

➧ *Gehen Sie folgendermaßen vor, um der Liste der Programme für die Sichere Umgebung ein Programm hinzuzufügen:*

1. Öffnen Sie das Programmhauptfenster.

2. Wählen Sie auf der linken Seite des Fensters den Abschnitt **Programmkontrolle**.

3. Klicken Sie im unteren Bereich des Fensters im Feld **Programme, die in der Sicheren Umgebung gestartet werden** auf den Link **Hinzufügen**.

4. Wählen Sie im Kontextmenü das erforderliche Programm aus. Bei Auswahl des Punkts **Durchsuchen** wird ein Fenster geöffnet, in dem der Pfad der ausführbaren Datei angegeben werden muss. Bei Auswahl des Punkts **Programme** wird eine Liste der momentan aktiven Programme geöffnet. Anschließend wird das Programmsymbol zu diesem Feld hinzugefügt.

   Um ein Programm aus der Liste für die Sichere Umgebung zu entfernen, markieren Sie es in der Liste und klicken Sie auf den Link **Löschen**.

MODUS AUSWÄHLEN: PROGRAMM STARTEN

In der Grundeinstellung können alle Programme, die auf dem Computer installiert sind, im gewöhnlichen Modus oder in der Sicheren Umgebung gestartet werden. Wenn ein Programm zur Liste der Programme, die in der Sicheren Umgebung gestartet werden sollen, hinzugefügt wird, kann der Modus **Immer im sicheren Modus starten** dafür festgelegt werden. Das bedeutet, dass das Programm unabhängig von der Startmethode (mit Hilfe der Standardmittel von Microsoft Windows oder mit Mitteln von Kaspersky Internet Security) in der Sicheren Umgebung gestartet wird.

Es wird davon abgeraten, den Modus **Immer im sicheren Modus starten** für Systemprogramme und -Utilities zu verwenden, weil dadurch die Funktionsfähigkeit des Betriebssystems gestört werden kann.

➧ *Gehen Sie folgendermaßen vor, damit ein Programm unabhängig von der Startmethode immer in der Sicheren Umgebung gestartet wird:*

1. Öffnen Sie das Programmhauptfenster.

2. Wählen Sie auf der linken Seite des Fensters den Abschnitt **Programmkontrolle**.

3. Wählen Sie im unteren Bereich das Symbol des gewünschten Programms aus.

4. Öffnen Sie mit Hilfe der rechten Maustaste das Kontextmenü.

5. Wählen Sie den Punkt **Immer im sicheren Modus starten**. Neben dem Menüpunkt wird nun ein Häkchen angezeigt.

   Damit der Start im gewöhnlichen Modus für das Programm verfügbar ist, wählen Sie erneut diesen Punkt aus.

MODUS AUSWÄHLEN: DATEN DER SICHEREN UMGEBUNG LÖSCHEN

Beim Start eines Programms in der Sicheren Umgebung erfolgen alle Veränderungen, die durch die Arbeit eines Programms verursacht werden, nur innerhalb der virtuellen Umgebung. In der Grundeinstellung sind beim nächsten Start eines Programms alle während einer Sitzung in der Sicheren Umgebung vorgenommenen Änderungen und gespeicherten Dateien wieder verfügbar.

Wenn die Daten der Sicheren Umgebung nicht mehr benötigt werden, können sie bereinigt werden (s. S. 88).

Wenn Sie nicht möchten, dass für ein bestimmtes Programm beim nächsten Start die in der Sicheren Umgebung vorgenommenen Änderungen verfügbar sind, können Sie den Modus **Daten der Sicheren Umgebung beim Beenden löschen** dafür festlegen. Das bedeutet, dass Änderungen, die während der Programmsitzung vorgenommen werden, verloren gehen. Programme, die in diesem Modus gestartet werden, erhalten das Symbol .

Gehen Sie folgendermaßen vor, damit die Daten der Sicheren Umgebung jedes Mal gelöscht werden, wenn ein Programm beendet wird:

1. Öffnen Sie das Programmhauptfenster.
2. Wählen Sie auf der linken Seite des Fensters den Abschnitt **Programmkontrolle**.
3. Wählen Sie im unteren Bereich das Symbol des gewünschten Programms aus.
4. Öffnen Sie mit Hilfe der rechten Maustaste das Kontextmenü.
5. Wählen Sie den Punkt **Daten der Sicheren Umgebung beim Beenden löschen**. Neben dem Menüpunkt wird nun ein Häkchen angezeigt und das Programmsymbol in der Liste der Programme, die in der Sicheren Umgebung gestartet werden, erhält das Symbol .

   Damit Daten, die während einer Programmsitzung in der Sicheren Umgebung gespeichert wurden, nicht gelöscht werden, wenn ein Programm beendet wird, klicken Sie erneut auf diesen Menüpunkt.

GEMEINSAMEN ORDNER VERWENDEN

Bei der Arbeit in der Sicheren Umgebung erfolgen alle Veränderungen, die durch die Arbeit eines Programms verursacht werden, nur innerhalb der virtuellen Umgebung und wirken sich nicht auf die normale Umgebung aus. Dateien, die in der Sicheren Umgebung gespeichert werden, gelangen auf diese Weise nicht in die normale Umgebung.

Damit die Dateien, mit denen ein Benutzer in der Sicheren Umgebung gearbeitet hat, auch in der normalen Umgebung zur Verfügung stehen, ist in Kaspersky Internet Security die Möglichkeit zur Verwendung eines *Gemeinsamen Ordners der Sicheren Umgebung* vorgesehen. Alle Dateien, die bei der Arbeit in der Sicheren Umgebung in diesem Ordner gespeichert werden, stehen in der normalen Umgebung zur Verfügung.

Der gemeinsame Ordner ist ein Ordner auf der Festplatte, der bei der Installation von Kaspersky Internet Security angelegt wird.

Der gemeinsame Ordner wird bei der Programminstallation im Ordner *%AllUsersProfile%\Application Data\Kaspersky Lab\SandboxShared* erstellt und sein Ort kann nicht verändert werden.

Im Explorer von Microsoft Windows besitzt der gemeinsame Ordner das Symbol . Auf den Ordner kann auch aus dem Hauptfenster von Kaspersky Internet Security zugegriffen werden.

Gehen Sie folgendermaßen vor, um den gemeinsamen Ordner aus dem Hauptfenster von Kaspersky Internet Security zu öffnen:

1. Öffnen Sie das Programmhauptfenster.
2. Wählen Sie auf der linken Seite des Fensters den Abschnitt **Programmkontrolle**.
3. Klicken Sie auf den Link **Gemeinsamer Ordner**. Dadurch wird der Ordner in einem Standardfenster von Microsoft Windows geöffnet.

SICHEREN UMGEBUNG BEREINIGEN

Wenn es erforderlich ist, die Daten der Sicheren Umgebung zu löschen oder wenn für alle gestarteten Programme die aktuellen Parameter in der Umgebung von Microsoft Windows wiederhergestellt werden sollen, kann die Bereinigung der Sicheren Umgebung verwendet werden.

Bevor Sie die Daten der Sicheren Umgebung bereinigen, sollten Sie sich vergewissern, dass alle Informationen, die künftig noch benötigt werden, im gemeinsamen Ordner gespeichert wurden. Andernfalls werden die Daten gelöscht und können nicht wiederhergestellt werden.

Gehen Sie folgendermaßen vor, um die Daten der Sicheren Umgebung zu bereinigen:

1. Öffnen Sie das Programmhauptfenster.
2. Wählen Sie auf der linken Seite des Fensters den Abschnitt **Programmkontrolle**.
3. Klicken Sie im unteren Bereich des Fensters im Feld **Programme, die in der Sicheren Umgebung gestartet werden** auf den Link **Leeren**.
4. Bestätigen Sie im folgenden Fenster mit der Schaltfläche **OK** das Löschen der Daten oder klicken Sie auf die Schaltfläche **Abbrechen**, damit keine Bereinigung erfolgt.

FIREWALL

Die *Firewall* ist eine Komponente von Kaspersky Internet Security, die die sichere Arbeit in lokalen Netzwerken und im Internet gewährleistet. Sie führt die Filterung der gesamten Netzwerkaktivität durch, wozu zwei Arten von Regeln dienen: *Regeln für Programme* und *Paketregeln*.

Die Firewall analysiert die Parameter der Netzwerke, die Sie mit Ihrem Computer verbinden. Wenn die Anwendung im interaktiven Funktionsmodus arbeitet (s. Abschnitt "Interaktiven Schutzmodus verwenden" auf S. 160), fragt die Firewall Sie bei der ersten Verbindung nach dem Status des verbundenen Netzwerks. Wenn der interaktive Funktionsmodus deaktiviert wurde, ermittelt die Firewall den Status, wozu Netzwerktyp, Adressenbereich und anderen Merkmale verwendet werden. Abhängig vom Netzwerkstatus verwendet die Firewall unterschiedliche Regeln zur Filterung der Netzwerkaktivität.

➡ *Gehen Sie folgendermaßen vor, um die Funktionsparameter des Proaktiven Schutzes zu ändern:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Firewall** aus.
3. Klicken Sie für die ausgewählte Komponente auf die Schaltfläche **Einstellungen**.
4. Ändern Sie im folgenden Fenster auf den Registerkarten **Filterregeln** und **Netzwerke** die Funktionsparameter der **Firewall**.

IN DIESEM ABSCHNITT

Netzwerkstatus ändern 89

Adressenbereich eines Netzwerks erweitern 90

Modus für die Benachrichtigung über Veränderungen eines Netzwerks auswählen 91

Erweiterte Einstellungen für die Firewall 91

Firewall-Regeln 92

NETZWERKSTATUS ÄNDERN

Alle Netzwerkverbindungen auf Ihrem Computer werden von der Firewall kontrolliert. Die Firewall weist jeder Verbindung einen bestimmten Status zu und verwendet abhängig vom ihrem Netzwerkstatus unterschiedliche Regeln für die Filterung der Netzwerkaktivität.

Wenn eine Verbindung mit einem neuen Netzwerk erfolgt, erscheint auf dem Bildschirm eine Meldung der Firewall (s. S. 214). Um eine Methode für die Filterung der Netzwerkaktivität auszuwählen, muss dem gefundenen Netzwerk ein *Status* zugewiesen werden. Folgende folgenden Statusvarianten stehen zur Auswahl:

- **Öffentliches Netzwerk (Internet)**. Dieser Status wird für Netzwerke empfohlen, die nicht durch Antiviren-Programme, Firewalls, Filter usw. geschützt werden (z.B. für Netzwerke in Internet-Cafés). Für die Benutzer solcher Netzwerke ist der Zugriff auf Dateien und Drucker, die sich auf Ihrem Computer befinden, gesperrt. Selbst wenn Sie einen gemeinsamen Ordner erstellt haben, erhalten Benutzer eines Netzwerks, das diesen Status besitzt, keinen Zugriff auf die darin enthaltenen Informationen. Auch wenn Sie den Remote-Zugriff auf den Arbeitsplatz erlaubt haben, können Benutzer eines solchen Netzwerks nicht darauf zugreifen. Die Filterung der Netzwerkaktivität richtet sich für jedes Programm nach den für dieses Programm bestehenden Regeln. Dieser Status wird standardmäßig dem Internet zugewiesen.

- **Lokales Netzwerk**. Dieser Status wird für Netzwerke empfohlen, deren Benutzer Sie den Zugriff auf Dateien und Drucker auf Ihrem Computer gewähren möchten (beispielsweise für interne Firmennetzwerke oder private Netzwerke).

- **Vertrauenswürdiges Netzwerk**. Es wird empfohlen, diesen Status nur für ein absolut sicheres Netzwerk zu verwenden, in dem Computer keine Angriffe und Versuche zum unerlaubten Datenzugriff drohen. Bei Auswahl dieser Variante wird jede beliebige Netzwerkaktivität im Rahmen dieses Netzwerks erlaubt.

Die Arten der Netzwerkaktivität, die für Netzwerke mit einem bestimmten Status erlaubt sind, hängen von den Parametern der standardmäßig gültigen Paketregeln ab. Sie können diese Regeln ändern.

Der Netzwerkstatus bestimmt die Auswahl der Regeln, die für die Filterung der diesem Netzwerk entsprechenden Aktivität verwendet werden.

Gehen Sie folgendermaßen vor, um den Status einer Netzwerkverbindung zu ändern:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.

2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Firewall** aus.

3. Klicken Sie für die ausgewählte Komponente auf die Schaltfläche **Einstellungen**.

4. Wählen Sie im folgenden Fenster auf der Registerkarte **Netzwerke** eine aktive Netzwerkverbindung aus und klicken Sie auf den Link **Ändern**.

5. Wählen Sie im folgenden Fenster auf der Registerkarte **Eigenschaften** den erforderlichen Status aus der Dropdown-Liste aus.

ADRESSENBEREICH EINES NETZWERKS ERWEITERN

Jedem Netzwerk entsprechen ein oder mehrere IP-Adressenbereiche. Wenn Sie eine Verbindung mit einem Netzwerk herstellen, auf dessen Subnetze über einen Router zugegriffen wird, können Sie die darüber verfügbaren Subnetze manuell hinzufügen.

Beispiel: Sie stellen eine Verbindung zu dem Netzwerk eines Büros Ihrer Firma her und möchten, dass die Filterregeln für das Büro, mit dem die Direktverbindung erfolgt, und für die über dieses Netzwerk erreichbaren Büros, einheitlich sind.

Erkundigen Sie sich beim Netzwerkadministrator nach den Adressenbereichen dieser Büros und fügen Sie diese hinzu.

Gehen Sie folgendermaßen vor, um den Adressenbereichs eines Netzwerks zu erweitern:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.

2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Firewall** aus.

3. Klicken Sie für die ausgewählte Komponente auf die Schaltfläche **Einstellungen**.

4. Wählen Sie im folgenden Fenster auf der Registerkarte **Netzwerke** eine aktive Netzwerkverbindung aus und klicken Sie auf den Link **Ändern**.

5. Klicken Sie im folgenden Fenster auf der Registerkarte **Eigenschaften** im Block **Zusätzliche Subnetze** auf den Link **Hinzufügen**.

6. Legen Sie im folgenden Fenster **IP-Adresse** eine IP-Adresse oder eine Adressenmaske fest.

MODUS FÜR DIE BENACHRICHTIGUNG ÜBER VERÄNDERUNGEN EINES NETZWERKS AUSWÄHLEN

Die Parameter von Netzwerkverbindungen können sich im Verlauf der Arbeit ändern. Sie können sich über folgende Veränderungen informieren lassen:

- Bei Netzwerkverbindung.
- Bei Veränderung der Korrespondenz zwischen MAC-Adresse und IP-Adresse. Diese Meldung erscheint, wenn die IP-Adresse eines Netzwerkcomputers verändert wird.
- Beim Erscheinen einer MAC-Adresse. Diese Meldung erscheint, wenn ein neuer Computer zu einem Netzwerk hinzugefügt wird.

Gehen Sie folgendermaßen vor, um die Benachrichtigung über Veränderungen der Parameter einer Netzwerkverbindung zu aktivieren:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Firewall** aus.
3. Klicken Sie für die ausgewählte Komponente auf die Schaltfläche **Einstellungen**.
4. Wählen Sie im folgenden Fenster auf der Registerkarte **Netzwerke** eine aktive Netzwerkverbindung aus und klicken Sie auf den Link **Ändern**.
5. Aktivieren Sie im folgenden Fenster auf der Registerkarte **Erweitert** die Kontrollkästchen für die Ereignisse, über die eine Meldung erfolgen soll.

ERWEITERTE EINSTELLUNGEN FÜR DIE FIREWALL

Zu den erweiterten Einstellungen für die Firewall zählen:

- Aktiven FTP-Modus zulassen. Der aktive Modus sieht vor, dass für eine Verbindung zwischen Server und Client auf dem Client-Computer ein Port geöffnet wird, mit dem der Server eine Verbindung aufbauen kann (im Unterschied zum passiven Modus, in dem der Client selbst eine Verbindung mit dem Server aufbaut). In diesem Modus ist es möglich, den zu öffnenden Port festzulegen. Der Mechanismus funktioniert auch, wenn eine Verbotsregel besteht. Der aktive FTP-Modus ist standardmäßig erlaubt.
- Verbindungen werden blockiert, wenn keine Aktionsanfrage möglich ist (wenn die Programmoberfläche nicht geladen ist). Es kann festgelegt werden, dass die Arbeit der Firewall nicht angehalten wird, während die Oberfläche von Kaspersky Internet Security nicht geladen ist. Diese Aktion wird standardmäßig ausgeführt.
- Firewall erst ausschalten, wenn System vollständig heruntergefahren wird Dieser Parameter erlaubt es, dass die Arbeit der Firewall erst beendet wird, wenn das System vollständig heruntergefahren wird. Diese Aktion wird standardmäßig ausgeführt.

Gehen Sie folgendermaßen vor, um zusätzliche Parameter für die Firewall festzulegen:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Firewall** aus.
3. Klicken Sie für die ausgewählte Komponente auf die Schaltfläche **Einstellungen**.
4. Klicken Sie im folgenden Fenster auf der Registerkarte **Filterregeln** auf die Schaltfläche **Erweitert**.

5. Vergewissern Sie sich, dass im folgenden Fenster **Erweitert** die entsprechenden Kontrollkästchen aktiviert sind.

FIREWALL-REGELN

Eine *Regel* für die Firewall besteht aus einer Aktion, die von der Firewall ausgeführt wird, wenn ein Verbindungsversuch mit bestimmten Parametern erkannt wird: Richtung und Protokoll für die Datenübertragung, Adressenbereich und Ports mit denen die Verbindung erfolgt.

Die Firewall arbeitet mit zwei Arten von Regeln:

- *Paketregeln* (s. Abschnitt "Paketregel erstellen" auf S. 92) dienen zur Definition von Beschränkungen für die Pakete und Datenströme, wobei die Programme keine Rolle spielen.

- *Programmregeln* (s. Abschnitt "Regel für ein Programm erstellen" auf S. 93) dienen zur Definition von Beschränkungen für die Netzwerkaktivität eines konkreten Programms. Solche Regeln erlauben es, die Filterung genau anzupassen, wenn beispielsweise ein bestimmter Typ von Datenströmen für manche Programme erlaubt, für andere aber verboten werden soll.

Paketregeln besitzen eine höhere Priorität als Regeln für Programme. Wenn für eine Art der Netzwerkaktivität gleichzeitig Paketregeln und Regeln für Programme vorhanden sind, wird diese Netzwerkaktivität nach den Paketregeln verarbeitet.

SIEHE AUCH

Paketregel erstellen 92

Regel für ein Programm erstellen 93

Assistent für neue Regeln 94

Aktion auswählen, die von einer Regel ausgeführt werden soll 94

Parameter eines Netzwerkdiensts anpassen 95

Adressenbereich auswählen 95

PAKETREGEL ERSTELLEN

Paketregeln beziehen sich meistens auf die eingehende Netzwerkaktivität bestimmter Ports mit den Protokollen TCP und UDP und regulieren die Filterung von ICMP-Nachrichten.

Eine *Paketregel* besteht aus einer Kombination von Bedingungen und Aktionen, die mit Paketen und Datenströmen ausgeführt werden, wenn die festgelegten Bedingungen erfüllt sind.

Wenn Sie Paketregeln erstellen, beachten Sie bitte, dass diese eine höhere Priorität besitzen als Regeln für Programme.

In den Bedingungen einer Regel können Netzwerkdienst und Netzwerkadresse angegeben werden. Als Netzwerkadresse kann eine IP-Adresse verwendet oder ein Netzwerkstatus angegeben werden. Im zweiten Fall werden die Adressen aller Netzwerke verwendet, mit denen momentan eine Verbindung besteht und die den betreffenden Status besitzen.

➡ *Gehen Sie folgendermaßen vor, um eine neue Paketregel zu erstellen:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.

2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Firewall** aus.

3. Klicken Sie für die ausgewählte Komponente auf die Schaltfläche **Einstellungen**.

4. Wählen Sie im folgenden Fenster auf der Registerkarte **Filterregeln** den Block **Paketregeln** aus und klicken Sie auf den Link **Hinzufügen**.

5. Passen Sie im Fenster **Netzwerkregel** die Parameter der Regel an.

6. Legen Sie die Priorität der neuen Regel fest.

Nachdem eine Regel erstellt wurde, können ihre Einstellungen geändert werden oder die Regel kann gelöscht werden. Dazu dienen die entsprechenden Links im unteren Bereich der Registerkarte. Um eine Regel zu deaktivieren, entfernen Sie das Kontrollkästchen neben ihrem Namen.

REGEL FÜR EIN PROGRAMM ERSTELLEN

Die Firewall analysiert die Aktivität aller Programme, die auf Ihrem Computer gestartet werden. Abhängig von der Risikobewertung wird jedes Programm bei seinem ersten Start einer der folgenden Gruppen zugeordnet:

- **Vertrauenswürdig**. Programmen dieser Gruppe wird unabhängig vom Netzwerkstatus jede Netzwerkaktivität erlaubt.

- **Schwach beschränkt**. Programmen dieser Gruppe wird im automatischen Modus jede Netzwerkaktivität erlaubt. Im interaktiven Modus erscheint eine Meldung auf dem Bildschirm, mit deren Hilfe Sie die Verbindung zulassen oder verbieten können, oder mit Hilfe des Assistenten (s. Abschnitt "Assistent für neue Regeln" auf S. 94) eine Regel für das Programm erstellen können.

- **Stark beschränkt**. Programmen dieser Gruppe wird im automatischen Modus jede Netzwerkaktivität erlaubt. Im interaktiven Modus erscheint eine Meldung auf dem Bildschirm, mit deren Hilfe Sie die Verbindung zulassen oder verbieten können, oder mit Hilfe des Assistenten (s. Abschnitt "Assistent für neue Regeln" auf S. 94) eine Regel für das Programm erstellen können.

- **Nicht vertrauenswürdig**. Programmen dieser Gruppe wird jede Netzwerkaktivität verboten.

Regeln können sowohl für eine ganze Gruppe als auch für ein bestimmtes Programm einer Gruppe geändert werden. Außerdem können zusätzliche Regeln erstellt werden, um die Filterung der Netzwerkaktivität genauer anzupassen.

Benutzerdefinierte Regeln für bestimmte Programme besitzen eine höhere Priorität als Regeln, die zu einer Gruppe gehören.

Nach der Analyse der Programmaktivität erstellt die Firewall Regeln, die den Zugriff des Programms auf Netzwerke mit einem bestimmten Status regulieren. Sie können zusätzliche Regeln erstellen, um die Netzwerkaktivität von Kaspersky Internet Security flexibel zu steuern.

➡ *Gehen Sie folgendermaßen vor, um eine Regel für ein Programm zu erstellen:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.

2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Firewall** aus.

3. Klicken Sie für die ausgewählte Komponente auf die Schaltfläche **Einstellungen**.

4. Wählen Sie im folgenden Fenster auf der Registerkarte **Filterregeln** eine Gruppe von Regeln für ein Programm aus und klicken Sie auf den Link **Hinzufügen**.

5. Passen Sie im Fenster **Netzwerkregel** die Parameter der Regel an.

6. Legen Sie die Priorität der neuen Regel fest.

Nachdem eine Regel erstellt wurde, können ihre Einstellungen geändert werden oder die Regel kann gelöscht werden. Dazu dienen die entsprechenden Links im unteren Bereich der Registerkarte. Um eine Regel zu deaktivieren, entfernen Sie das Kontrollkästchen neben ihrem Namen.

ASSISTENT FÜR NEUE REGELN

Wenn eine Regel ausgelöst wird, für die die Aktion **Aktion erfragen** gilt (diese Aktion wird standardmäßig für Programme der Gruppe (s. Abschnitt "Programmgruppen" auf S. 76) **Schwach beschränkt** oder **Stark beschränkt** festgelegt), erscheint eine Meldung (s. S. 213) auf dem Bildschirm. In der Meldung kann eine der folgenden Varianten für das weitere Vorgehen ausgewählt werden:

- **Erlauben**.
- **Verbieten**.
- **Regel erstellen**. Bei Auswahl dieser Variante wird der *Assistent für neue Regeln* gestartet, der Sie dabei unterstützt, eine Regel für die Netzwerkaktivität der Anwendung zu erstellen.

Wenn eine Regel ausgelöst wurde, kann die Aktion in **Erlauben** oder **Verbieten** geändert werden. Dazu muss das Kontrollkästchen **Speichern für dieses Programm** aktiviert werden.

Der Assistent besteht aus einer Reihe von Fenstern (Schritten). Zur Navigation zwischen den Fenstern dienen die Schaltfläche **Zurück** und der Link **Weiter**, zum Abschluss des Assistenten der Link **Fertig**. Die Arbeit des Assistenten kann auf einer beliebigen Etappe durch Klick auf die Schaltfläche **Abbrechen** beendet werden.

AKTION AUSWÄHLEN, DIE VON EINER REGEL AUSGEFÜHRT WERDEN SOLL

Wenn eine Regel ausgelöst wird, führt die Firewall eine der folgenden Aktionen mit einem Paket oder einem Datenstrom aus:

- **Erlauben**.
- **Blockieren**.
- **Nach Programmregeln bearbeiten**. In diesem Fall wird die Verarbeitung eines Pakets oder eines Datenstroms mit Hilfe der Paketregel abgebrochen. Auf die Verbindung werden die Regeln für Programme angewendet.

Wenn Informationen über Verbindungsversuche und über Aktionen der Firewall in einem Bericht aufgezeichnet werden sollen, aktivieren Sie den Modus **Protokollieren.**

Gehen Sie folgendermaßen vor, um die Aktion zu ändern, die von der Firewall ausgeführt werden soll:

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Firewall** aus.
3. Klicken Sie für die ausgewählte Komponente auf die Schaltfläche **Einstellungen**.
4. Klicken Sie im folgenden Fenster auf der Registerkarte **Filterregeln** auf den Link **Hinzufügen**.
5. Wählen Sie im folgenden Fenster **Netzwerkregel** im Block **Aktion** eine Aktion aus.

PARAMETER EINES NETZWERKDIENSTS ANPASSEN

Die Parameter, die eine Netzwerkaktivität charakterisieren, für die eine Regel erstellt wird, werden durch einem *Netzwerkdienst* beschrieben. Ein Netzwerkdienst besitzt folgende Parameter:

- *Name*. Dieser Text wird in der Liste der verfügbaren Netzwerkdienste angezeigt.
- *Richtung*. Die Firewall kontrolliert Verbindungen in folgende Richtung:
  - **Eingehend**. Die Regel wird auf Datenpakete angewandt, die von Ihrem Computer empfangen werden. Sie wird nicht in den Regeln für Programme verwendet.
  - **Eingehend (Strom)**. Die Regel wird auf eine Netzwerkverbindung angewandt, die von einem Remote-Computer geöffnet wird.
  - **Eingehend / Ausgehend**. Die Regel wird sowohl auf ein eingehendes als auch auf ein ausgehendes Paket / Datenstrom angewandt, unabhängig davon, von welchem Computer (von Ihrem oder einem Remote-Computer) die Netzwerkverbindung initiiert wurde.
  - **Ausgehend**. Die Regel wird auf Datenpakete angewandt, die von Ihrem Computer gesendet werden. Sie wird nicht in den Regeln für Programme verwendet.
  - **Ausgehend (Strom)**. Die Regel wird nur für eine Netzwerkverbindung angewandt, die von Ihrem Computer geöffnet wird.
- *Protokoll*. Die Firewall kontrolliert Verbindungen der Protokolle TCP, UDP, ICMP, ICMPv6, IGMP und GRE. Wenn Sie ICMP oder ICMPv6 als Protokoll gewählt haben, können Sie Typ und Code des ICMP-Pakets angeben.

Die Regeln für Programme kontrollieren nur Verbindungen mit den Protokollen TCP und UDP.

- *Remoteports und lokale Ports*. Für die Protokolle TCP und UDP können Sie die Ports Ihres Computers und eines Remote-Computers festlegen, zwischen denen eine Verbindung kontrolliert werden soll.

Zum Lieferumfang von Kaspersky Internet Security gehören Netzwerkdienste, die die am häufigsten verwendeten Netzwerkverbindungen beschreiben. Beim Erstellen von Firewall-Regeln können Sie einen der vordefinierten Netzwerkdienste auswählen oder einen neuen erstellen.

➡ *Gehen Sie folgendermaßen vor, um die Parameter einer Netzwerkverbindung, die mit der Regel verarbeitet werden soll, anzupassen:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Firewall** aus.
3. Klicken Sie für die ausgewählte Komponente auf die Schaltfläche **Einstellungen**.
4. Klicken Sie im folgenden Fenster auf der Registerkarte **Filterregeln** auf den Link **Hinzufügen**.
5. Klicken Sie im folgenden Fenster **Netzwerkregel** im Block **Netzwerkdienst** auf den Link **Hinzufügen**.
6. Passen Sie im folgenden Fenster **Netzwerkdienst** die Parameter der Netzwerkverbindung an.

ADRESSENBEREICH AUSWÄHLEN

Eine Firewall-Regel wird auf folgende Kategorien von Netzwerkadressen angewandt:

- **Beliebige Adresse** – Die Regel wird auf eine beliebige IP-Adresse angewendet.

- **Subnetzadressen mit Status** – Die Regel findet Anwendung auf die IP-Adressen aller Netzwerke, mit denen momentan eine Verbindung besteht und die den entsprechenden Status besitzen.

- **Adressen aus folgender Gruppe** – Die Regel wird auf IP-Adressen angewandt, die dem angegebenen Bereich angehören.

Gehen Sie folgendermaßen vor, um den Bereich der IP-Adressen anzugeben, auf die eine Regel angewandt werden soll:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.

2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Firewall** aus.

3. Klicken Sie für die ausgewählte Komponente auf die Schaltfläche **Einstellungen**.

4. Klicken Sie im folgenden Fenster auf der Registerkarte **Filterregeln** auf den Link **Hinzufügen**.

5. Geben Sie im folgenden Fenster **Netzwerkregel** im Block **Adressen** einen Adressenbereich an:

   a. Wählen Sie in der Liste einen Netzwerkstatus aus, wenn Sie die Variante **Subnetzadressen mit Status** festgelegt haben.

   b. Wählen Sie eine der vorhandenen Adressengruppen aus, wenn Sie die Variante **Adressen aus folgender Gruppe** gewählt haben. Falls die Adressenbereiche der vorhandenen Gruppen ungeeignet sind, erstellen Sie eine Gruppe. Klicken Sie dazu im unteren Bereich des Blocks auf den Link **Hinzufügen** und geben Sie im folgenden Fenster **Netzwerkadressen** die Adressen an, die zu der Gruppe gehören.

PROAKTIVER SCHUTZ

Kaspersky Internet Security schützt nicht nur vor bekannten, sondern auch vor neuen Bedrohungen, über die keine Informationen in den Datenbanken von Kaspersky Internet Security vorhanden sind. Diese Möglichkeit wird durch die speziell entwickelten Komponente *Proaktiver Schutz* gewährleistet.

Die präventiven Technologien, auf denen der Proaktive Schutz beruht, erlauben es, einen Zeitverlust zu vermeiden und eine neue Bedrohung zu neutralisieren, bevor sie auf Ihrem Computer Schaden verursachen kann. Im Unterschied zu den reaktiven Technologien, bei denen die Analyse auf Basis von Einträgen der Datenbanken von Kaspersky Internet Security erfolgt, identifizieren die Präventivtechnologien eine neue Bedrohung auf Ihrem Computer nach den Aktionsfolgen, die von einem bestimmten Programm ausgeführt werden. Wenn aufgrund der Aktivitätsanalyse die Aktionsfolge eines Programms als verdächtig eingestuft wird, sperrt Kaspersky Internet Security seine Aktivität.

Die Aktivitätsanalyse erstreckt sich auf alle Programme, einschließlich der Programme, die von der Komponente Programmkontrolle der Gruppe **Vertrauenswürdig** zugeordnet wurden (auf S. 74). Für diese Programme können Sie die Benachrichtigungen des Proaktiven Schutzes deaktivieren.

Im Unterschied zur Komponente Programmkontrolle reagiert der Proaktive Schutz genau auf bestimmte Aktionsfolgen eines Programms.

Gehen Sie folgendermaßen vor, um die Funktionsparameter des Proaktiven Schutzes zu ändern:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Proaktiver Schutz** aus.
3. Passen Sie die Parameter der ausgewählten Komponente entsprechend an.

IN DIESEM ABSCHNITT

Liste der gefährlichen Aktivität verwenden 97

Kontrollregel für gefährliche Aktivität ändern 98

Gruppe mit vertrauenswürdigen Programmen erstellen 99

Kontrolle über Systembenutzerkonten 99

LISTE DER GEFÄHRLICHEN AKTIVITÄT VERWENDEN

Beachten Sie, dass die Einstellungen für die Aktivitätskontrolle in Kaspersky Internet Security unterschiedlich sind, je nachdem, ob die Anwendung auf einem Computer mit einem der Betriebssysteme Microsoft Windows XP Professional x64 Edition, Microsoft Windows Vista oder Microsoft Windows Vista x64 installiert ist als auf einem Computer mit einem anderen Betriebssystem.

Besonderheiten der Einstellungen für die Aktivitätskontrolle für Programme unter dem Betriebssystem Microsoft Windows XP

Die Aktivität der Anwendungen auf Ihrem Computer wird von Kaspersky Internet Security kontrolliert. Der Proaktive Schutz reagiert auf eine bestimmte Folge von Programmaktionen. Werden beispielsweise Aktionen erkannt, bei denen sich ein bestimmtes Programm auf eine Netzwerkressource, in den Autostart-Ordner oder in die Systemregistrierung kopiert, und anschließend seine Kopien versendet, so handelt es sich mit hoher Wahrscheinlichkeit um einen Wurm. Als gefährliche Aktionsfolgen zählen außerdem:

- Aktionen, die für trojanische Programme charakteristisch sind.
- Versuche zum Abfangen von Tastatureingaben.
- Versteckte Installation von Treibern.
- Versuche zum Ändern des Betriebssystemkerns.
- Versuche zum Erstellen versteckter Objekte und Prozesse mit negativem PID-Wert.
- Veränderung der HOSTS-Datei.
- Versuche zum Eindringen in andere Prozesse.
- Auftreten von Prozessen, die die Eingabe / Ausgabe von Daten umleiten.
- Versuche zum Senden von DNS-Anfragen.

Die Liste der gefährlichen Aktivitäten wird beim Update von Kaspersky Internet Security automatisch ergänzt und kann nicht verändert werden. Allerdings können Sie die Kontrolle bestimmter Typen gefährlicher Aktivität deaktivieren.

Gehen Sie folgendermaßen vor, um die Kontrolle bestimmter Typen gefährlicher Aktivität zu deaktivieren:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Proaktiver Schutz** aus.
3. Klicken Sie für die ausgewählte Komponente auf die Schaltfläche **Einstellungen**.
4. Deaktivieren Sie im folgenden Fenster **Proaktiver Schutz** das Kontrollkästchen neben dem Namen der Aktivität, die nicht kontrolliert werden soll.

Besonderheiten der Einstellungen für die Aktivitätskontrolle für Programme unter den Betriebssystemen Microsoft Windows XP Professional x64 Edition, Microsoft Windows Vista oder Microsoft Windows Vista x64

Wenn der Computer unter einem der oben genannten Betriebssysteme läuft, werden nicht alle Ereignisse kontrolliert. Dies hängt mit Besonderheiten dieser Betriebssysteme zusammen. Beispielsweise werden folgende Arten von Ereignissen nicht kontrolliert: *Eindringen in anderen Prozess*, *Senden von Daten über vertrauenswürdige Programme*, *Verdächtige Aktivität im System*, *Zugriff auf geschützten Speicher*.

KONTROLLREGEL FÜR GEFÄHRLICHE AKTIVITÄT ÄNDERN

Die Liste der gefährlichen Aktivitäten wird beim Update von Kaspersky Internet Security automatisch ergänzt und kann nicht verändert werden. Sie können:

- Kontrolle einer bestimmten Aktivität deaktivieren (s. S. 97).
- eine Regel ändern, nach welcher der Proaktive Schutz beim Fund einer gefährlichen Aktivität vorgeht.
- Liste von Ausnahmen (s. S. 175) erstellen, indem Sie die Anwendungen festlegen, deren Aktivität Sie nicht für gefährlich halten.

Gehen Sie folgendermaßen vor, um eine Regel zu ändern:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Proaktiver Schutz** aus.

3. Klicken Sie für die ausgewählte Komponente auf die Schaltfläche **Einstellungen**.

4. Wählen Sie im folgenden Fenster **Proaktiver Schutz** im Block **Ereignisse** das Ereignis aus, für das die Regel geändert werden soll.

5. Legen Sie für das ausgewählte Ereignis mit Hilfe der Links im Block mit der Regelbeschreibung die entsprechenden Parameter fest:

   - Klicken Sie auf den Link mit der geltenden Aktion und wählen Sie im folgenden Fenster **Aktion auswählen** die entsprechende Aktion aus.

   - Klicken Sie auf den Link für das geltende Intervall (Es wird nicht für alle Aktivitätsarten ein Intervall angegeben) und legen Sie im folgenden Fenster **Versteckte Prozesse erkennen** ein Intervall fest, mit dem die Suche nach versteckten Prozessen ausgeführt werden soll.

   - Klicken Sie auf den Link Ein / Aus, um festzulegen, ob ein Bericht über die ausgeführte Operation erstellt werden soll.

GRUPPE MIT VERTRAUENSWÜRDIGEN PROGRAMMEN ERSTELLEN

Programme, die von der Komponente Programmkontrolle der Gruppe (s. Abschnitt "Programmgruppen" auf S. 76) **Vertrauenswürdig** zugeordnet werden, stellen keine Gefahr für das System dar. Trotzdem wird ihre Aktivität auch von der Komponente Proaktiver Schutz kontrolliert.

Es besteht die Möglichkeit, eine Liste mit vertrauenswürdigen Programmen anzulegen, deren Aktivität nicht vom Proaktiven Schutz überwacht werden soll. Programme, die eine digitale Signatur besitzen oder in der Datenbank von Kaspersky Security Network enthalten sind, können als vertrauenswürdig eingestuft werden.

Gehen Sie folgendermaßen vor, damit der Proaktive Schutz Programme, die eine digitale Signatur besitzen und / oder in der Datenbank von Kaspersky Security Network enthalten sind, als vertrauenswürdig betrachtet und nicht über ihre Aktivität informiert:

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.

2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Proaktiver Schutz** aus.

3. Aktivieren Sie für die ausgewählte Komponente im Block **Vertrauenswürdige Programme** das Kontrollkästchen ☑ **Mit digitaler Signatur** und / oder das Kontrollkästchen ☑ **Die in der Datenbank von Kaspersky Security Network enthalten sind**.

KONTROLLE ÜBER SYSTEMBENUTZERKONTEN

Benutzerkonten regulieren den Zugriff auf das System und definieren den Benutzer und seine Arbeitsumgebung. Dadurch werden Beschädigungen des Betriebssystems oder der Daten anderer Benutzer verhindert. Systemprozesse sind Prozesse, die vom Systembenutzerkonto gestartet wurden.

Gehen Sie folgendermaßen vor, damit Kaspersky Internet Security nicht nur Benutzerprozesse, sondern auch die Aktivität von Systemprozessen überwacht:

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.

2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Proaktiver Schutz** aus.

3. Aktivieren Sie für die ausgewählte Komponente im Block **Erweitert** das Kontrollkästchen ☑ **Systembenutzerkonten kontrollieren**.

SCHUTZ VOR NETZWERKANGRIFFEN

Der *Schutz vor Netzwerkangriffen* wird beim Hochfahren des Betriebssystems gestartet und überwacht den eingehenden Datenverkehr auf für Netzwerkangriffe charakteristische Aktivität. Wenn ein Angriffsversuch auf Ihren Computer erkannt wird, blockiert Kaspersky Internet Security jede Art von Netzwerkaktivität des angreifenden Computers. In der Grundeinstellung dauert die Blockade eine Stunde. Auf dem Bildschirm Meldung (s. Abschnitt "Meldungen" auf S. 207) über den versuchten Netzwerkangriff. Die Meldung enthält Informationen über den angreifenden Computer.

Beschreibungen der momentan bekannten Netzwerkangriffe (s. Abschnitt "Arten der erkennbaren Netzwerkangriffe" auf S. 100) und entsprechende Abwehrmethoden sind in den Datenbanken von Kaspersky Internet Security enthalten. Die Liste der Angriffe, die der Schutz vor Netzwerkangriffen erkennt, wird im Rahmen des Updates (s. Abschnitt "Update" auf S. 151) der Datenbanken aktualisiert.

IN DIESEM ABSCHNITT

Angreifende Computer sperren 100

Arten der erkennbaren Netzwerkangriffe 100

ANGREIFENDE COMPUTER SPERREN

In der Grundeinstellung blockiert der Schutz von Netzwerkangriffen (s. S. 100) die Aktivität eines angreifenden Computers für eine Stunde.

- *Gehen Sie folgendermaßen vor, um den Zeitraum, für den ein angreifender Computer gesperrt werden soll, zu ändern:*

  1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
  2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Schutz vor Netzwerkangriffen** aus.
  3. Aktivieren Sie für die ausgewählte Komponente das Kontrollkästchen **Angreifenden Computer zur Sperrliste hinzufügen für** und geben Sie die Sperrdauer an.

- *Gehen Sie folgendermaßen vor, um einen angreifenden Computer freizugeben:*

  1. Öffnen Sie das Programmhauptfenster und öffnen Sie das Programmhauptfenster und wählen Sie den Abschnitt **Schutz-Center**.
  2. Klicken Sie auf der rechten Seite des Fensters im Abschnitt **Arbeit im Netzwerk** auf den Link **Netzwerkmonitor**.
  3. Wählen Sie im folgenden Fenster auf der Registerkarte **Blockierte Computer** einen blockierten Computer aus und klicken Sie auf den Link **Freigeben**.

ARTEN DER ERKENNBAREN NETZWERKANGRIFFE

Heutzutage existiert einen Vielzahl unterschiedlicher Arten von Netzwerkangriffen, die sowohl Schwachstellen des Betriebssystems, als auch installierte System- und Anwendungsprogramme ausnutzen.

Um rechtzeitig für die Sicherheit des Computers zu sorgen, ist es wichtig zu wissen, welche Arten von Netzwerkangriffen ihm drohen können. Die bekannten Netzwerkangriffe lassen sich bedingt in drei große Gruppen unterteilen:

1. *Scannen von Ports* – Diese Bedrohungsart stellt getrennt betrachtet keinen Angriff dar, sondern geht diesem voraus, weil sie eine der effektivsten Methoden ist, Informationen über einen Remote-Computer zu erhalten. Die Methode besteht darin, die von Netzwerkdiensten auf dem angegriffenen Computer verwendeten UDP/TCP-Ports zu scannen, um deren Status (geschlossene oder offene Ports) zu ermitteln.

   Das Scannen von Ports gibt Aufschluss darüber, welche Angriffstypen für ein bestimmtes System am meisten Erfolg versprechen. Außerdem verleihen die aus dem Scannen resultierenden Informationen ("Abdruck" des Systems) dem Angreifer eine Vorstellung vom Typ des Betriebssystems auf dem entfernten Computer. Dadurch lässt sich die Art der relevanten Angriffe weiter einkreisen und damit die zum Ausführen der Angriffe notwendige Zeit verkürzen. Außerdem können die für das Betriebssystem spezifischen Sicherheitslücken ausgenutzt werden.

2. *DoS-Angriffe* oder Angriffe, die zur Dienstverweigerung führen Das Ziel dieser Angriffe besteht darin, die Instabilität des angegriffenen Systems hervorzurufen oder es vollständig außer Gefecht zu setzen. Aufgrund solcher Angriffe können die betroffenen Informationsressourcen unzugänglich werden (z.B. gestörter Internetzugriff).

   Es gibt zwei Haupttypen von DoS-Angriffen:

   - Es werden spezielle Pakete an den angegriffenen Computer geschickt, die dieser nicht erwartet. Die Folge ist eine Überlastung oder ein Systemabsturz.

   - An den angegriffenen Computer wird innerhalb eines kurzen Zeitraums eine große Anzahl von Paketen geschickt, die dieser Computer nicht verarbeiten kann. Als Folge erschöpfen die Systemressourcen.

   Die folgenden Angriffe bieten gute Beispiele für diese Gruppe:

   - Der Angriff *Ping of death* besteht im Senden eines ICMP-Pakets, dessen Größe den zulässigen Wert von 64 KB überschreitet. Dieser Angriff kann zum Absturz bestimmter Betriebssysteme führen.

   - Bei dem Angriff *Land* wird an einen offenen Port Ihres Computers eine Anfrage auf Verbindungsherstellung mit sich selbst gesendet. Der Angriff führt im angegriffenen Computer zu einer Endlosschleife, was eine stark erhöhte Prozessorbelastung zur Folge hat und bei bestimmten Betriebssystemen zum Absturz führen kann.

   - Bei dem Angriff *ICMP Flood* wird eine große Anzahl von ICMP-Paketen an Ihren Computer gesendet Da der Computer auf jedes eintreffende Paket reagieren muss, kommt es zu einer erheblichen Erhöhung der Prozessorauslastung.

   - Bei dem Angriff *SYN Flood* wird eine große Menge von Verbindungsanfragen an Ihren Computer gesendet. Das System reserviert für jede dieser Verbindungen bestimmte Ressourcen, wodurch es seine Ressourcen vollständig verbraucht und nicht mehr auf andere Verbindungsversuche reagiert.

3. *Angriffe zur "Übernahme"* - Diese Angriffe zielen auf die "Übernahme" des Systems ab. Dies ist der gefährlichste Angriffstyp, weil das System bei erfolgreichem Angriff dem Angreifer gegenüber vollkommen wehrlos ist.

   Dieser Angriff wird benutzt, um von einem Remote-Computer vertrauliche Informationen zu stehlen (beispielsweise Kreditkartennummern und Kennwörter). Ein weiteres Ziel kann darin bestehen, sich im System einzunisten, um später die Rechnerressourcen für die Zwecke des Angreifers zu nutzen (das angegriffene System wird in einem Zombie-Netzwerk oder als "Brückenkopf" für neue Angriffe verwendet).

   Zu dieser Gruppe gehört eine große Anzahl von Angriffen. Sie lassen sich abhängig von dem Betriebssystem, das auf einem Computer installiert ist, in drei Kategorien unterteilen: Angriffe auf Microsoft Windows-Systeme, Angriffe auf Unix-Systeme und eine allgemeine Gruppe für Netzwerkdienste, die in beiden Betriebssystemen verwendet werden.

   Die meistverbreiteten Arten von Angriffen, die auf Netzwerkdienste eines Betriebssystems zugreifen, sind:

   - *Angriffe mit dem Ziel des Pufferüberlaufs* – Ein Typ von Software-Schwachstellen, die auf fehlende (oder unzureichende) Kontrolle bei der Arbeit mit Daten (Array) zurückgehen. Dieser Typ von Schwachstellen gehört zu den ältesten und lässt sich am leichtesten von Angreifern ausnutzen.

- *Angriffe, die auf Fehlern in Formatzeilen beruhen* – Ein Typ von Software-Schwachstellen, die darauf beruhen, dass die Eingabeparameter von Formatfunktionen des Typs *printf()*, *fprintf()*, *scanf()* und anderer Standardbibliotheken der Sprache C unzureichend kontrolliert werden. Wenn diese Sicherheitslücke in einem Programm vorhanden ist, kann ein Angreifer die vollständige Kontrolle über das System übernehmen, wenn es ihm gelingt, speziell erstellte Anfragen zu senden.

Wenn solche Schwachstellen auf dem Benutzercomputer vorhanden sind, werden sie vom Detektionssystem für Angriffe in den gebräuchlichsten Netzwerkdiensten (FTP, POP3, IMAP) automatisch analysiert und verhindert ihre Verwendung.

Angriffe, die sich auf das Betriebssystem Microsoft Windows richten, beruhen auf der Verwendung von Sicherheitslücken der auf einem Computer installierten Software (beispielsweise solcher Programme wie Microsoft SQL Server, Microsoft Internet Explorer, Messenger, sowie Systemkomponenten, die über ein Netzwerk erreichbar sind: DCom, SMB, Wins, LSASS, IIS5).

Ein weiterer häufig anzutreffender Typ von Übernahmeangriffen ist die Verwendung unterschiedlicher Arten von schädlichen Skripts. Dazu zählen auch Skripts, die von Microsoft Internet Explorer verarbeitet werden, sowie die Variationen des Helkern-Wurms. Bei einem Helkern-Angriff werden spezielle UDP-Pakete mit ausführbarem schädlichem Code an einen entfernten Computer gesendet.

ANTI-SPAM

Anti-Spam ist eine spezielle Komponente von Kaspersky Internet Security, die unerwünschte E-Mails (Spam) erkennt und sie nach den Regeln Ihres Mailprogramms verarbeitet, um bei der Arbeit mit elektronischer Post wertvolle Zeit zu sparen.

Anti-Spam verwendet einen lernfähigen Algorithmus (s. Abschnitt "Algorithmus für die Arbeit der Komponente" auf S. 104), mit dem die Komponente mit der Zeit genauer zwischen Spam und nützlicher E-Mails unterscheiden kann. Als Datenquelle für den Algorithmus dient der Inhalt einer E-Mail. Eine Voraussetzung für die effektive Unterscheidung zwischen Spam und nützlichen E-Mails, ist ein Training von Anti-Spam (s. Abschnitt "Anti-Spam-Training" auf S. 106).

Es wird ausdrücklich empfohlen, sich über den Algorithmus für die Arbeit von Anti-Spam zu informieren!

Anti-Spam wird als Erweiterungsmodul in folgende Mailprogramme integriert:

- Microsoft Office Outlook (s. Abschnitt "Spam-Verarbeitung in Microsoft Office Outlook anpassen" auf S. 119).
- Microsoft Outlook Express (Windows Mail) (s. Abschnitt "Spam-Verarbeitung in Microsoft Outlook Express (Windows Mail) anpassen" auf S. 120).
- The Bat! (s. Abschnitt "Spam-Verarbeitung in The Bat! anpassen" auf S. 121).
- Thunderbird (s. Abschnitt "Spam-Verarbeitung in Thunderbird anpassen" auf S. 122).

Legen Sie Listen für erlaubte (s. S. 113) und verbotene (s. S. 111) Absender an, um für Anti-Spam festzulegen, von welchen Adressen nützliche E-Mails bzw. Spam-Mails zu erwarten sind. Außerdem kann Anti-Spam eine Nachricht auf das Vorhandensein von Phrasen aus den Listen für erlaubte (s. S. 114) und verbotene (s. S. 112) Phrasen, sowie aus der Liste für anstößige (s. S. 112) Ausdrücke analysieren.

Anti-Spam erlaubt die Anzeige von E-Mails auf dem Server (s. Abschnitt "Filterung von E-Mails auf dem Server. Mail-Manager" auf S. 117) und das Löschen unerwünschter Nachrichten, ohne sie auf Ihren Computer herunterzuladen.

Gehen Sie folgendermaßen vor, um die Funktionsparameter von Anti-Spam anzupassen:

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Anti-Spam** aus.
3. Klicken Sie für die ausgewählte Komponente auf die Schaltfläche **Einstellungen**.
4. Passen Sie die Parameter der Komponente entsprechend an.

IN DIESEM ABSCHNITT

Algorithmus für die Arbeit der Komponente 104

Anti-Spam-Training 106

Sicherheitsstufe ändern 109

Untersuchungsmethode auswählen 110

Liste mit vertrauenswürdigen Adressen erstellen 111

Liste mit verbotenen Absendern erstellen 111

Liste mit verbotenen Phrasen erstellen 112

Liste mit anstößigen Phrasen erstellen 112

Liste der erlaubten Absender erstellen 113

Liste mit erlaubten Phrasen erstellen 114

Liste mit erlaubten Absendern importieren 114

Faktor für Spam und potentiellen Spam festlegen 115

Algorithmus zur Spam-Erkennung auswählen 116

Zusätzliche Merkmale für die Spam-Filterung verwenden 116

Markierung zum Betreff einer Nachricht hinzufügen 117

Filterung von E-Mails auf dem Server. Mail-Manager 117

Nachrichten für Microsoft Exchange Server von der Untersuchung ausschließen 118

Aktionen für unerwünschte E-Mails 118

Standardparameter für Anti-Spam wiederherstellen 122

ALGORITHMUS FÜR DIE ARBEIT DER KOMPONENTE

Die Arbeit der Komponente Anti-Spam besteht aus zwei Etappen:

1. Anwendung von strengen Kriterien für die Filterung einer Nachricht. Diese Kriterien ermöglichen es, schnell festzustellen, ob eine Nachricht Spam ist oder nicht. Anti-Spam weist der Nachricht den Status *Spam* oder *Kein Spam*, die Untersuchung wird beendet und die Nachricht zur Bearbeitung an das Mailprogramm weitergeleitet (siehe unten: Schritte 1 – 5).

2. Analyse von E-Mails, die nach den strengen Kriterien der vorhergehenden Schritte nicht eingestuft werden konnten. Solche Nachrichten lassen sich nicht eindeutig als Spam bewerten. Deshalb muss Anti-Spam die *Wahrscheinlichkeit* berechnen, mit der es sich bei einer Nachricht um Spam handelt.

Der Algorithmus für die Arbeit von Anti-Spam umfasst folgende Schritte:

1. Es wird geprüft, ob die Absenderadresse einer E-Mail auf den Listen für erlaubte und verbotene Absender steht.

- Wenn die Absenderadresse in der Liste mit erlaubten Adressen steht, erhält die Nachricht den Status *Kein Spam*.

- Wenn die Absenderadresse in der Liste mit verbotenen Adressen steht, erhält die Nachricht den Status *Spam*.

2. Wurde die Nachricht mit Hilfe von Microsoft Exchange Server gesendet und die Untersuchung solcher Nachrichten ist deaktiviert (s. S. 118), dann erhält sie den Status *Kein Spam*.

3. Die Nachricht wird auf das Vorhandensein von Zeilen aus der Liste mit erlaubten Phrasen (s. S. 114) analysiert. Wenn mindestens eine Zeile aus dieser Liste gefunden wird, erhält die Nachricht den Status *Kein Spam*. Dieser Schritt wird standardmäßig übersprungen.

4. Die Nachricht wird auf das Vorhandensein von Zeilen aus der Liste mit verbotenen Phrasen (s. S. 112) analysiert. Wenn in der Nachricht Wörter aus dieser Liste gefunden werden, erhöht sich die Wahrscheinlichkeit, dass es sich um Spam handelt. Wenn die berechnete Wahrscheinlichkeit über dem festgelegten Wert (s. S. 115) liegt, erhält die Nachricht den Status *Spam* oder *potentieller Spam*. Die Nachricht wird auch auf das Vorhandensein von Zeilen aus der Liste mit zensierten Phrasen (s. S. 112) analysiert. Dieser Schritt wird standardmäßig übersprungen.

5. Wenn der Nachrichtentext eine Adresse enthält, die in der Datenbank von verdächtigen oder Phishing-Adressen (s. S. 110) steht, erhält die Nachricht den Status *Spam*.

6. Die Nachricht wird mit Hilfe heuristischer Regel analysiert. Wenn aufgrund dieser Analyse in E-Mails typische Spam-Merkmale gefunden werden, erhöht sich die Wahrscheinlichkeit, dass es sich um Spam handelt.

7. Die Nachricht wird mit Hilfe der GSG-Technologie analysiert. Dabei überprüft Anti-Spam die in der E-Mail enthaltenen Bilder. Wenn in den Bildern typische Spam-Merkmale gefunden werden, erhöht sich die Wahrscheinlichkeit, dass es sich um Spam handelt.

8. Dokumente des Formats *.rtf*, die an eine E-Mail angehängt sind, werden analysiert. Anti-Spam sucht in angehängten Dokumenten nach typischen Spam-Merkmalen. Zum Abschluss der Analyse berechnet Anti-Spam, wie stark sich die Wahrscheinlichkeit erhöht hat, dass es sich bei der Nachricht um Spam handelt. Diese Technologie ist standardmäßig deaktiviert.

9. Das Vorhandensein zusätzlicher Merkmale (s. S. 116), die für Spam charakteristisch sind, wird überprüft. Jede Übereinstimmung erhöht die Wahrscheinlichkeit, dass es sich um Spam handelt.

10. Wenn zuvor das Anti-Spam-Training ausgeführt wurde, wird die Nachricht mit Hilfe der iBayes-Technologie untersucht. Der lernfähige iBayes-Algorithmus berechnet die Wahrscheinlichkeit, mit der es sich bei der Nachricht um Spam handelt. Dazu wird analysiert, wie häufig im Text der Nachricht typische Spam-Phrasen vorkommen.

Das Ergebnis der Nachrichtenanalyse ergibt die Wahrscheinlichkeit, mit der die E-Mail als Spam gilt. Spammer verbessern die Tarnung von Spam ständig. Deshalb erreicht die rechnerische Wahrscheinlichkeit nur selten den festgelegten Wert (s. Abschnitt "Faktor für Spam und potentiellen Spam festlegen" auf S. 115). Zur zuverlässigen Filterung des E-Mail-Aufkommens verwendet Anti-Spam zwei Parameter:

- *Spam-Faktor* – Wahrscheinlichkeitswert, bei dessen Überschreitung eine E-Mail als *Spam* gilt. Wenn die Wahrscheinlichkeit unter diesem Wert liegt, verleiht Anti-Spam der Nachricht den Status *potentieller Spam*.

- *Faktor für potentiellen Spam* – Wahrscheinlichkeitswert, bei dessen Überschreitung eine E-Mail als potentieller Spam gilt. Wenn die Wahrscheinlichkeit unter diesem Wert liegt, stuft Anti-Spam die Nachricht als nützlich ein.

In Abhängigkeit von den Werten, die für die Faktoren für Spam und potentiellen Spam festgelegt wurden, erhalten Nachrichten den Status *Spam* oder *potentieller Spam*. Außerdem wird den Nachrichten im Feld **Betreff** dem zugewiesenen Status entsprechend die Markierung **[!! SPAM]** oder **[?? Probable Spam]** hinzugefügt. Anschließend werden sie nach den Regeln (s. Abschnitt "Aktionen für unerwünschte E-Mails" auf S. 118) verarbeitet, die Sie für Ihr Mailprogramm festgelegt haben.

ANTI-SPAM-TRAINING

Eines der Werkzeuge zur Spam-Erkennung ist der lernfähige iBayes-Algorithmus. Dieser Algorithmus entscheidet auf Basis der in einer Nachricht enthaltenen Phrasen darüber, welcher Status ihr zugewiesen wird. Bevor begonnen wird, mit dem iBayes-Algorithmus zu arbeiten, ist ein Training mit Zeilenmustern aus nützlichen E-Mails und aus Spam-Mails erforderlich.

Es existieren mehrere Methoden für das Training von Anti-Spam:

- Verwendung eines Trainingsassistenten (s. Abschnitt "Training mit Hilfe des Trainingsassistenten" auf S. 106) (Pakettraining). Das Training mit Hilfe des Trainingsassistenten sollte ganz zu Beginn der Arbeit mit Anti-Spam erfolgen.
- Anti-Spam-Training mit ausgehenden E-Mails (s. Abschnitt "Anti-Spam-Training mit ausgehenden E-Mails" auf S. 107).
- Training während der Arbeit mit der E-Mail-Korrespondenz (s. Abschnitt "Training mit Hilfe eines Mailprogramms" auf S. 108), wozu die speziellen Schaltflächen in der Symbolleiste des Mailprogramms oder die Menüpunkte dienen.
- Training bei der Arbeit mit den Anti Spam-Berichten (s. Abschnitt "Training mit Berichten" auf S. 109).

TRAINING MIT HILFE DES TRAININGSASSISTENTEN

Der Trainingsassistent erlaubt es, ein Anti-Spam-Training im Paketmodus vorzunehmen. Dazu ist es erforderlich, die Ordner der Mailprogramme Microsoft Office Outlook und Microsoft Outlook Express (Windows Mail) anzugeben, in denen sich Spam und nützliche E-Mails befinden.

Für die korrekte Spam-Erkennung ist es erforderlich, das Training mit mindestens 50 nützlichen E-Mails und 50 Spam-Mustern vorzunehmen. Der iBayes-Algorithmus funktioniert nur, wenn die genannten Aktionen ausgeführt wurden.

Um Zeit zu sparen, wird das Training mit dem Assistenten auf 50 Nachrichten aus jedem gewählten Ordner beschränkt.

Der Assistent besteht aus einer Reihe von Fenstern (Schritten). Zur Navigation zwischen den Fenstern dienen die Schaltflächen **Zurück** und **Weiter**, zum Abschluss des Assistenten die Schaltfläche **Beenden**. Die Arbeit des Assistenten kann auf einer beliebigen Etappe durch Klick auf die Schaltfläche **Abbrechen** beendet werden.

➡ *Gehen Sie folgendermaßen vor, den Assistenten zu starten:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Anti-Spam** aus.
3. Klicken Sie für die ausgewählte Komponente im Block **Anti-Spam-Training** auf die Schaltfläche **Trainieren**.

Beim Training mit nützlichen E-Mails werden die Absenderadressen zur Liste der erlaubten Absender hinzugefügt.

➡ *Gehen Sie folgendermaßen vor, damit die Absenderadressen nicht in die Liste mit erlaubten Adressen aufgenommen werden:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Anti-Spam** aus.
3. Klicken Sie für die ausgewählte Komponente auf die Schaltfläche **Einstellungen**.

4. Aktivieren Sie im folgenden Fenster auf der Registerkarte **Allgemein** im Block **Folgende Nachrichten als nützlich einstufen** das Kontrollkästchen **Von erlaubten Absendern** und klicken Sie auf die Schaltfläche **Auswählen**.

5. Deaktivieren Sie im folgenden Fenster **Liste der erlaubten Absender** das Kontrollkästchen **Beim Anti-Spam-Training im Mailprogramm Adressen von erlaubten Absendern hinzufügen**.

SIEHE AUCH

Training mit Berichten.....109

Training mit Hilfe eines Mailprogramms 108

Anti-Spam-Training mit ausgehenden E-Mails 107

ANTI-SPAM-TRAINING MIT AUSGEHENDEN E-MAILS

Sie können Anti-Spam mit 50 ausgehenden E-Mails trainieren. Die Empfängeradressen dieser Nachrichten werden automatisch zur Liste der erlaubten Absender hinzugefügt.

Gehen Sie folgendermaßen vor, um Anti-Spam mit ausgehenden E-Mails zu trainieren:

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.

2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Anti-Spam** aus.

3. Klicken Sie für die ausgewählte Komponente auf die Schaltfläche **Einstellungen**.

4. Aktivieren Sie im folgenden Fenster auf der Registerkarte **Erweitert** im Block **Ausgehende E-Mails** das Kontrollkästchen **Mit ausgehenden E-Mails trainieren**.

Gehen Sie folgendermaßen vor, damit die Absenderadressen nicht in die Liste mit erlaubten Adressen aufgenommen werden:

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.

2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Anti-Spam** aus.

3. Klicken Sie für die ausgewählte Komponente auf die Schaltfläche **Einstellungen**.

4. Aktivieren Sie im folgenden Fenster auf der Registerkarte **Allgemein** im Block **Folgende Nachrichten als nützlich einstufen** das Kontrollkästchen **Von erlaubten Absendern** und klicken Sie auf die Schaltfläche **Auswählen**.

5. Deaktivieren Sie im folgenden Fenster **Liste der erlaubten Absender** das Kontrollkästchen **Beim Anti-Spam-Training im Mailprogramm Adressen von erlaubten Absendern hinzufügen**.

SIEHE AUCH

Training mit Hilfe des Trainingsassistenten 106

Training mit Berichten.....109

Training mit Hilfe eines Mailprogramms 108

TRAINING MIT HILFE EINES MAILPROGRAMMS

Das Training von Anti-Spam während der Arbeit mit der E-Mail-Korrespondenz erfolgt unter Verwendung spezieller Elemente auf der Benutzeroberfläche Ihres Mailprogramms.

Die Schaltflächen für das Anti-Spam-Training erscheinen auf der Programmoberfläche von Microsoft Office Outlook und Microsoft Outlook Express (Windows Mail), nachdem Kaspersky Internet Security installiert wurde.

Gehen Sie folgendermaßen vor, um Anti-Spam mit Hilfe eines Mailprogramms zu trainieren:

1. Starten Sie das Mailprogramm.
2. Wählen Sie eine Nachricht aus, mit deren Hilfe Sie Anti-Spam trainieren möchten.
3. Führen Sie - abhängig davon, welchen Mail-Client Sie verwenden - folgende Aktionen aus:
   - Klicken Sie in der Symbolleiste von Microsoft Office Outlook auf die Schaltfläche **Spam** oder **Kein Spam**.
   - Klicken Sie in der Symbolleiste von Microsoft Office Outlook (Windows Mail) auf die Schaltfläche **Spam** oder **Kein Spam**.
   - Verwenden Sie im Mailprogramm The Bat! die dafür vorgesehenen Punkte **Als Junk klassifizieren** und **Als Nicht-Junk klassifizieren** im Menü **Extras**.
   - Verwenden Sie in der Symbolleiste von Mozilla Thunderbird die Schaltfläche **Spam/Kein Spam**.

Nachdem eine der oben genannten Aktionen ausgewählt wurde, führt Anti-Spam mit der ausgewählten Nachricht ein Training durch. Wenn Sie mehrere Nachrichten markieren, erfolgt das Training mit allen ausgewählten E-Mails.

Wenn eine Nachricht als nützlich markiert wird, wird die Absenderadresse zur Liste der erlaubten Absender hinzugefügt.

Gehen Sie folgendermaßen vor, damit die Absenderadressen nicht in die Liste mit erlaubten Adressen aufgenommen werden:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Anti-Spam** aus.
3. Klicken Sie für die ausgewählte Komponente auf die Schaltfläche **Einstellungen**.
4. Aktivieren Sie im folgenden Fenster auf der Registerkarte **Allgemein** im Block **Folgende Nachrichten als nützlich einstufen** das Kontrollkästchen ☑ **Von erlaubten Absendern** und klicken Sie auf die Schaltfläche **Auswählen**.
5. Deaktivieren Sie im folgenden Fenster **Liste der erlaubten Absender** das Kontrollkästchen ☑ **Beim Anti-Spam-Training im Mailprogramm Adressen von erlaubten Absendern hinzufügen**.

Wenn Sie gleichzeitig mehrere Nachrichten markieren oder sicher sind, dass ein bestimmter Ordner nur Nachrichten einer Gruppe (Spam oder Kein Spam) enthält, kann zum Training der Komponente die Paketmethode mit Hilfe des Trainingsassistenten benutzt werden (s. Abschnitt "Anti-Spam-Training" auf S. 106).

SIEHE AUCH

Anti-Spam-Training mit ausgehenden E-Mails 107

Training mit Hilfe des Trainingsassistenten 106

Training mit Berichten 109

TRAINING MIT BERICHTEN

Es besteht die Möglichkeit, Anti-Spam auf Basis von Berichten zu trainieren. Die Berichte der Komponente erlauben Schlussfolgerungen über die Genauigkeit ihrer Einstellungen und bei Bedarf können bestimmte Anti-Spam-Parameter korrigiert werden.

Gehen Sie folgendermaßen vor, um eine bestimmte Nachricht als Spam oder Kein Spam zu markieren:

1. Öffnen Sie das Programmhauptfenster.
2. Gehen Sie mit Hilfe des Links **Bericht** in das Berichtsfenster von Kaspersky Internet Security.
3. Klicken Sie im folgenden Fenster auf der Registerkarte **Bericht** auf die Schaltfläche **Vollständiger Bericht**.
4. Wählen Sie für die Komponente **Anti-Spam** eine Nachricht aus, mit deren Hilfe das zusätzliche Training erfolgen soll.
5. Öffnen Sie das Kontextmenü für die Nachricht und wählen Sie eine der folgenden Aktionen aus:
   - **Als Spam markieren**.
   - **Als Kein Spam markieren**.
   - **Zur Liste der erlaubten Absender hinzufügen**.
   - **Zur Liste der erlaubten Absender hinzufügen**.

SIEHE AUCH

Anti-Spam-Training mit ausgehenden E-Mails 107

Training mit Hilfe des Trainingsassistenten 106

Training mit Hilfe eines Mailprogramms 108

SICHERHEITSSTUFE ÄNDERN

Anti-Spam verwendet zwei Kennziffern für die E-Mail-Filterung:

- *Spam-Faktor* – Wahrscheinlichkeitswert, bei dessen Überschreitung eine E-Mail als Spam gilt. Wenn die Wahrscheinlichkeit unter diesem Wert liegt, verleiht Anti-Spam der Nachricht den Status *potentieller Spam*.
- *Faktor für potentiellen Spam* – Wahrscheinlichkeitswert, bei dessen Überschreitung eine E-Mail als potentieller Spam gilt. Wenn die Wahrscheinlichkeit unter diesem Wert liegt, stuft Anti-Spam die Nachricht als nützlich ein.

Die Spezialisten von Kaspersky Lab haben drei Sicherheitsstufen vordefiniert.

- **Hoch**. Diese Sicherheitsstufe sollte verwendet werden, wenn Sie sehr viel Spam erhalten, z.B. bei Verwendung eines kostenlosen Maildiensts. Bei Auswahl dieser Stufe kann die Wahrscheinlichkeit steigen, dass nützliche Post als Spam eingestuft wird.

- **Mittel**. Diese Sicherheitsstufe gilt für die meisten Situationen als empfohlen.

- **Niedrig**. Diese Sicherheitsstufe sollte verwendet werden, wenn Sie nur selten Spam erhalten, z.B. bei der Arbeit in einer geschützten Umgebung des internen Firmen-Mailsystem. Bei Auswahl dieser Stufe kann die Wahrscheinlichkeit sinken, dass nützliche Post als Spam oder potentieller Spam eingestuft wird.

Gehen Sie folgendermaßen vor, um die festgelegte Sicherheitsstufe für Anti-Spam zu ändern:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.

2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Anti-Spam** aus.

3. Legen Sie die erforderliche Sicherheitsstufe für die gewählte Komponente fest.

UNTERSUCHUNGSMETHODE AUSWÄHLEN

Die Untersuchungsmethoden beziehen sich hier auf die Untersuchung der in E-Mails enthaltenen Links auf ihre Zugehörigkeit zur Liste mit verbotenen Webadressen und / oder zur Liste der Phishing-Webadressen.

Durch die Untersuchung von Links auf die Zugehörigkeit zur Liste der Phishing-Adressen lassen sich Phishing-Angriffe abwehren, die in der Regel die Form von E-Mails besitzen, die scheinbar von finanziellen Institutionen stammen und Links auf deren Webseiten enthalten. Die Nachricht fordert dazu auf, einem Link zu folgen und auf der betreffenden Seite vertrauliche Informationen wie beispielsweise eine Kreditkartennummer oder Benutzername und Kennwort für die persönliche Internet-Banking-Seite einzugeben, auf der finanzielle Operationen erfolgen können.

Ein häufiges Beispiel für Phishing-Angriffe ist der Brief einer Bank, bei der Sie Kunde sind, mit einem Link zu deren offizieller Internetseite. Wenn Sie dem Link folgen, gelangen Sie auf eine Webseite, die eine genaue Kopie der Bankseite darstellt und im Browser sogar deren Adresse anzeigen kann, obwohl Sie sich in Wirklichkeit auf einer fiktiven Seite befinden. Alle Aktionen, die Sie auf dieser Seite ausführen, werden verfolgt und können zum Diebstahl Ihres Geldes missbraucht werden.

Gehen Sie folgendermaßen vor, um die in E-Mails enthaltenen Links mit der Datenbank für verdächtige Adressen zu untersuchen:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.

2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Anti-Spam** aus.

3. Klicken Sie für die ausgewählte Komponente auf die Schaltfläche **Einstellungen**.

4. Aktivieren Sie im folgenden Fenster auf der Registerkarte **Allgemein** im Block **Folgende Nachrichten als Spam einstufen** das Kontrollkästchen ☑ **Mit Links aus der Datenbank für verdächtige Webadressen**.

Gehen Sie folgendermaßen vor, um die in E-Mails enthaltenen Links mit der Datenbank für Phishing-Adressen zu untersuchen:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.

2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Anti-Spam** aus.

3. Klicken Sie für die ausgewählte Komponente auf die Schaltfläche **Einstellungen**.

4. Aktivieren Sie im folgenden Fenster auf der Registerkarte **Allgemein** im Block **Folgende Nachrichten als Spam einstufen** das Kontrollkästchen ☑ **Mit Links aus der Datenbank für Phishing-Webadressen**.

LISTE MIT VERTRAUENSWÜRDIGEN ADRESSEN ERSTELLEN

Sie können eine Liste mit vertrauenswürdigen Adressen anlegen. Anti-Spam prüft, ob die Empfängeradresse zu dieser Liste gehört.

Gehen Sie folgendermaßen vor, um eine Liste mit vertrauenswürdigen Adressen anzulegen:

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Anti-Spam** aus.
3. Klicken Sie für die ausgewählte Komponente auf die Schaltfläche **Einstellungen**.
4. Aktivieren Sie im folgenden Fenster auf der Registerkarte **Allgemein** das Kontrollkästchen **Nicht an mich adressiert** und klicken Sie auf die Schaltfläche **Meine Adressen**.
5. Klicken Sie im folgenden Fenster **Meine Adressen** auf den Link **Hinzufügen**.
6. Geben Sie im folgenden Fenster **Maske für E-Mail-Adresse** die erforderlichen Adressen oder Adressenmasken an.

LISTE MIT VERBOTENEN ABSENDERN ERSTELLEN

Als Adresse können sowohl Adressen als auch Adressenmasken benutzt werden. Bei der Angabe einer Maske können die Zeichen ***** und **?** verwendet werden (wobei ***** für eine beliebige Zeichenfolge und das Zeichen **?** für ein beliebiges Einzelzeichen steht). Beispiele für Adressenmasken:

- *ivanov@test.ru*. E-Mail-Nachrichten von einem Absender mit dieser Adresse werden immer als Spam klassifiziert.
- **@test.ru*. E-Mails von allen Absendern der Maildomäne *test.ru* gelten als Spam. Beispiele: *petrov@test.ru*, *sidorov@test.ru*.
- *ivanov@**. Ein Absender mit diesem Namen sendet unabhängig von der Maildomäne nur Spam. Beispiele: *ivanov@test.ru*, *ivanov@mail.ru*.
- **@test**. Post von einem beliebigen Absender der Maildomäne *test* gilt als Spam. Beispiele: *ivanov@test.ru*, *petrov@test.com*.
- *ivan.*@test.???*. Mails von einem Absender, dessen Name mit *ivan.* beginnt und dessen Maildomäne mit *test* anfängt und mit drei beliebigen Zeichen endet, gilt immer als Spam. Beispiele: *ivan.ivanov@test.com*, *ivan.petrov@test.org*.

Gehen Sie folgendermaßen vor, um eine Liste mit verbotenen Absendern anzulegen und sie künftig bei der Arbeit zu verwenden:

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Anti-Spam** aus.
3. Klicken Sie für die ausgewählte Komponente auf die Schaltfläche **Einstellungen**.
4. Aktivieren Sie im folgenden Fenster auf der Registerkarte **Allgemein** im Block **Folgende Nachrichten als Spam einstufen** das Kontrollkästchen **Von verbotenen Absendern** und klicken Sie auf die Schaltfläche **Auswählen**.

5. Klicken Sie im folgenden Fenster **Liste der verbotenen Absender** auf den Link **Hinzufügen**.

6. Geben Sie im folgenden Fenster **Maske für E-Mail-Adresse** eine Adresse oder Maske an.

LISTE MIT VERBOTENEN PHRASEN ERSTELLEN

In der Liste der verbotenen Phrasen werden Schlüsselphrasen aus E-Mails gespeichert, die Sie für Spam halten. Die Liste wird manuell ergänzt.

Als Phrasen können Masken verwendet werden. Bei der Angabe einer Maske können die Zeichen ***** und **?** verwendet werden (wobei ***** für eine beliebige Zeichenfolge und das Zeichen **?** für ein beliebiges Einzelzeichen steht). Beispiele für Phrasen und Phrasenmasken:

- *Hallo Ivan!*. Eine Nachricht, die nur diesen Text enthält, gilt als Spam. Es wird davor gewarnt, solche Phrasen zu verwenden.
- *Hallo Ivan!**. Eine Nachricht, die mit der Zeile *Hallo Ivan!* beginnt, gilt als Spam.
- *Hallo *! *.* Eine Nachricht, die mit dem Grußwort *Hallo* beginnt und an einer beliebigen Stelle ein Ausrufezeichen enthält, gilt als Spam.
- ** Ivan? *.* Eine Nachricht, die sich an einen Benutzer mit dem Namen *Ivan* wendet, auf den ein beliebiges Zeichen folgt, gilt als Spam.
- ** Ivan\? **. Eine Nachricht, welche die Phrase *Ivan?* enthält, gilt als Spam.

Wenn die Zeichen * und ? in einer Phrase vorkommen, muss ihnen das neutralisierende Zeichen \ vorangestellt werden, damit Anti-Spam den Ausdruck korrekt interpretiert. In diesem Fall werden anstelle eines Zeichens zwei verwendet: *und \?.

➡ *Gehen Sie folgendermaßen vor, um eine Liste mit verbotenen Phrasen anzulegen:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.

2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Anti-Spam** aus.

3. Klicken Sie für die ausgewählte Komponente auf die Schaltfläche **Einstellungen**.

4. Aktivieren Sie im folgenden Fenster auf der Registerkarte **Allgemein** im Block **Folgende Nachrichten als Spam einstufen** das Kontrollkästchen ☑ **Mit verbotenen Phrasen** und klicken Sie auf die Schaltfläche **Auswählen**.

5. Klicken Sie im folgenden Fenster **Liste der verbotenen Phrasen** auf den Link **Hinzufügen**.

6. Geben Sie im folgenden Fenster **Verbotene Phrase** eine entsprechende Zeile oder Maske ein.

LISTE MIT ANSTÖßIGEN PHRASEN ERSTELLEN

Die Liste enthält anstößige Phrasen, deren Vorhandensein in einer Nachricht mit großer Wahrscheinlichkeit darauf hinweist, dass es sich um Spam handelt.

Im Lieferumfang von Kaspersky Internet Security befindet sich eine Liste mit anstößigen Phrasen, die Spezialisten von Kaspersky Lab erstellt haben. Sie können diese Liste ergänzen.

Als Phrasen können Masken verwendet werden. Bei der Angabe einer Maske können die Zeichen ***** und **?** verwendet werden (wobei ***** für eine beliebige Zeichenfolge und das Zeichen **?** für ein beliebiges Einzelzeichen steht).

Wenn die Zeichen * und ? in einer Phrase vorkommen, muss ihnen das neutralisierende Zeichen \ vorangestellt werden, damit Anti-Spam den Ausdruck korrekt interpretiert. In diesem Fall werden anstelle eines Zeichens zwei verwendet: *und \?.

Gehen Sie folgendermaßen vor, um die Liste der anstößigen Phrasen zu bearbeiten:

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Anti-Spam** aus.
3. Klicken Sie für die ausgewählte Komponente auf die Schaltfläche **Einstellungen**.
4. Aktivieren Sie im folgenden Fenster auf der Registerkarte **Allgemein** im Block **Folgende Nachrichten als Spam einstufen** das Kontrollkästchen **Mit verbotenen Phrasen** und klicken Sie auf die Schaltfläche **Auswählen**.
5. Aktivieren Sie im folgenden Fenster **Liste der verbotenen Phrasen** das Kontrollkästchen **Als verboten einstufen: anstößige Phrasen** und klicken Sie auf den Link **anstößige Phrasen**.
6. Lesen Sie im folgenden Fenster **Vereinbarung** den Vereinbarungstext. Wenn Sie den genannten Bedingungen zustimmen, aktivieren Sie das entsprechende Kontrollkästchen und klicken Sie auf **OK**.
7. Klicken Sie im folgenden Fenster **Liste der anstößigen Lexik** auf den Link **Hinzufügen**.
8. Geben Sie im folgenden Fenster **Verbotene Phrase** eine entsprechende Zeile oder Maske ein.

LISTE DER ERLAUBTEN ABSENDER ERSTELLEN

In der Liste mit erlaubten Absendern werden die Adressen der E-Mail-Absender jener E-Mails gespeichert, von denen Sie sicher sind, dass sie keinen Spam senden. Diese Liste wird beim Training der Komponente Anti-Spam automatisch ergänzt. Sie können diese Liste ändern:

Als Adresse können sowohl Adressen als auch Adressenmasken benutzt werden. Bei der Angabe einer Maske können die Zeichen ***** und **?** verwendet werden (wobei ***** für eine beliebige Zeichenfolge und das Zeichen **?** für ein beliebiges Einzelzeichen steht). Beispiele für Adressenmasken:

- *ivanov@test.ru.* E-Mail-Nachrichten von einem Absender mit dieser Adresse werden immer als nützliche Post klassifiziert.
- **@test.ru.* E-Mails von allen Absendern der Maildomäne *test.ru* gelten als nützlich. Beispiele: *petrov@test.ru*, *sidorov@test.ru*.
- *ivanov@*.* Ein Absender mit diesem Namen sendet unabhängig von der Maildomäne nur nützliche Post. Beispiele: *ivanov@test.ru*, *ivanov@mail.ru*.
- **@test*.* Post von einem beliebigen Absender der Maildomäne *test* gilt nicht als Spam. Beispiele: *ivanov@test.ru*, *petrov@test.com*.
- *ivan.*@test.???.* Mails von einem Benutzer, dessen Name mit *ivan.* beginnt und dessen Maildomäne mit *test* anfängt und mit drei beliebigen Zeichen endet, gilt immer als nützlich. Beispiele: *ivan.ivanov@test.com*, *ivan.petrov@test.org*.

Gehen Sie folgendermaßen vor, um eine Liste mit erlaubten Absendern zu erstellen:

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Anti-Spam** aus.

3. Klicken Sie für die ausgewählte Komponente auf die Schaltfläche **Einstellungen**.

4. Aktivieren Sie im folgenden Fenster auf der Registerkarte **Allgemein** im Block **Folgende Nachrichten als nützlich einstufen** das Kontrollkästchen **Von erlaubten Absendern** und klicken Sie auf die Schaltfläche **Auswählen**.

5. Klicken Sie im folgenden Fenster **Liste der erlaubten Absender** auf den Link **Hinzufügen**.

6. Geben Sie im folgenden Fenster **Maske für E-Mail-Adresse** eine Adresse oder Maske an.

LISTE MIT ERLAUBTEN PHRASEN ERSTELLEN

In der Liste mit den erlaubten Phrasen werden Schlüsselphrasen aus E-Mails, die Sie als nützliche Post markiert haben, gespeichert. Sie können eine solche Liste anlegen.

Als Phrasen können Masken verwendet werden. Bei der Angabe einer Maske können die Zeichen ***** und **?** verwendet werden (wobei ***** für eine beliebige Zeichenfolge und das Zeichen **?** für ein beliebiges Einzelzeichen steht). Beispiele für Phrasen und Phrasenmasken:

- *Hallo Ivan!.* Eine Nachricht, die nur diesen Text enthält, gilt als nützlich. Es wird davor gewarnt, solche Phrasen zu verwenden.
- *Hallo Ivan!**. Eine Nachricht, die mit der Zeile *Hallo Ivan!*, beginnt, gilt als nützlich.
- *Hallo *! **. Eine Nachricht, die mit dem Grußwort *Hallo* beginnt und an einer beliebigen Stelle ein Ausrufezeichen enthält, gilt nicht als Spam.
- ** Ivan? **. Eine Nachricht, die sich an einen Benutzer mit dem Namen *Ivan* wendet, auf den ein beliebiges Zeichen folgt, gilt nicht als Spam.
- ** Ivan\? **. Eine Nachricht, welche die Phrase *Ivan?* enthält, gilt als nützlich.

Wenn die Zeichen * und ? in einer Phrase vorkommen, muss ihnen das neutralisierende Zeichen \ vorangestellt werden, damit Anti-Spam den Ausdruck korrekt interpretiert. In diesem Fall werden anstelle eines Zeichens zwei verwendet: *und \?.

Gehen Sie folgendermaßen vor, um eine Liste mit erlaubten Phrasen anzulegen:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.

2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Anti-Spam** aus.

3. Klicken Sie für die ausgewählte Komponente auf die Schaltfläche **Einstellungen**.

4. Aktivieren Sie im folgenden Fenster auf der Registerkarte **Allgemein** im Block **Folgende Nachrichten als nützlich einstufen** das Kontrollkästchen **Mit erlaubten Phrasen** und klicken Sie auf die Schaltfläche **Auswählen**.

5. Klicken Sie im folgenden Fenster **Liste der erlaubten Phrasen** auf den Link **Hinzufügen**.

6. Geben Sie im folgenden Fenster **Erlaubte Phrase** eine entsprechende Zeile oder Maske an.

LISTE MIT ERLAUBTEN ABSENDERN IMPORTIEREN

Für Adressen aus der Liste erlaubter Absender ist der Import von Dateien im Format **.txt*, **.csv* oder eines Adressbuchs für Microsoft Office Outlook / Microsoft Outlook Express (Windows Mail) möglich.

Gehen Sie folgendermaßen vor, um eine Liste mit erlaubten Absendern zu importieren:

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.

2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Anti-Spam** aus.

3. Klicken Sie für die ausgewählte Komponente auf die Schaltfläche **Einstellungen**.

4. Aktivieren Sie im folgenden Fenster auf der Registerkarte **Allgemein** im Block **Folgende Nachrichten als nützlich einstufen** das Kontrollkästchen **Von erlaubten Absendern** und klicken Sie auf die Schaltfläche **Auswählen**.

5. Klicken Sie im folgenden Fenster **Liste der erlaubten Absender** auf den Link **Import**.

6. Wählen Sie im Kontextmenü eine Importquelle aus:

   - **Importieren aus Datei**. Bei Auswahl dieser Quelle wird ein Fenster zur Dateiauswahl geöffnet. Das Programm unterstützt den Import aus Dateien der Typen *.csv* und *.txt*.

   - **Importieren aus Adressbuch**. Bei Auswahl dieser Quelle Fenster zur Auswahl eines Adressbuchs geöffnet. Wählen Sie in diesem Fenster das gewünschte Adressbuch aus.

FAKTOR FÜR SPAM UND POTENTIELLEN SPAM FESTLEGEN

Die Kaspersky-Lab-Spezialisten sind bemüht, Anti-Spam optimal für die Erkennung von Spam und potentiellem Spam einzustellen.

Die Spam-Erkennung basiert auf der Verwendung moderner Filtertechnologien, die es erlauben, Anti-Spam so zu trainieren, dass er relativ genau zwischen Spam, potentiellem Spam und nützlichen E-Mails unterscheiden kann. Das Training beruht auf der Analyse einer bestimmten Anzahl von Nachrichten des Benutzers.

Das Anti-Spam-Training erfolgt mit Hilfe des Trainingsassistenten und beim Training in Mailprogrammen. Dabei erhält jedes Element, das als nützliche Post oder Spam erkannt wird, einen bestimmten Koeffizienten. Wenn eine E-Mail in Ihrer Mailbox eintrifft, untersucht Anti-Spam die Nachricht mit Hilfe der iBayes-Technologie auf das Vorhandensein von Elementen, die für Spam und nützliche Post charakteristisch sind. Die Koeffizienten für jedes Element, das als Spam (nützliche Post) gilt, werden summiert, und die Faktoren für Spam und potentiellen Spam werden errechnet.

Der Wert des Faktors für potentiellen Spam definiert einen Grenzwert, bei dessen Überschreitung eine Nachricht den Ergebnisstatus *Potentieller Spam* erhält. Wenn für die Arbeit von Anti-Spam die Stufe **Empfohlen** verwendet wird, wird jede E-Mail mit einem Faktor von über 60% als potentieller Spam eingestuft. E-Mails werden als nützlich betrachtet, wenn der Wert für diesen Faktor bei der Untersuchung unter 60% liegt. Sie können den vordefinierten Wert ändern.

Der Wert des Spam-Faktors definiert einen Grenzwert, bei dessen Überschreitung eine Nachricht den Ergebnisstatus *Spam* erhält. Jede Nachricht, deren Faktor über dem festgelegten Wert liegt, wird als Spam betrachtet. Für die **Empfohlene** Stufe beträgt der Spam-Faktor standardmäßig 90%. Das bedeutet, dass jede Nachricht mit einem Faktor von über 90% als Spam gilt. Sie können den vordefinierten Wert ändern.

Gehen Sie folgendermaßen vor, um die festgelegten Werte der Faktoren für Spam und potentiellen Spam zu ändern:

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.

2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Anti-Spam** aus.

3. Klicken Sie für die ausgewählte Komponente auf die Schaltfläche **Einstellungen**.

4. Passen Sie im folgenden Fenster auf der Registerkarte **Algorithmus** im Block **Spam-Faktor** die Faktoren für Spam und potentiellen Spam an.

ALGORITHMUS ZUR SPAM-ERKENNUNG AUSWÄHLEN

Die Spam-Analyse von E-Mails erfolgt unter Verwendung spezieller Erkennungsalgorithmen.

- **Heuristische Analyse**. Anti-Spam analysiert die Nachrichten mit Hilfe heuristischer Regeln. Die heuristische Analyse wird immer verwendet.
- **Grafikanalyse (GSG)**. Die GSG-Technologie wird von Anti-Spam verwendet, um Spam in Form von Bildern zu identifizieren.
- **Analyse von angehängten Dokumenten im Format .rtf**. Anti-Spam analysiert die an Nachrichten angehängten Dokumente auf das Vorhandensein von Spam-Merkmalen.
- **Lernfähiger Algorithmus zur Textanalyse (iBayes)**. Der iBayes-Algorithmus ermittelt, ob eine E-Mail nützlich oder unerwünscht ist. Dazu wird analysiert, wie häufig im Text einer E-Mail Wörter verwendet werden, die für Spam typisch sind. Vor dem Beginn der Arbeit ist ein Training (s. Abschnitt "Anti-Spam-Training" auf S. 106) des iBayes-Algorithmus erforderlich.

Gehen Sie folgendermaßen vor, um bei der E-Mail-Analyse einen Spam-Erkennungsalgorithmus zu verwenden / nicht zu verwenden:

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Anti-Spam** aus.
3. Klicken Sie für die ausgewählte Komponente auf die Schaltfläche **Einstellungen**.
4. Aktivieren / deaktivieren Sie im folgenden Fenster auf der Registerkarte **Algorithmus** im Block **Erkennungsalgorithmen** die entsprechenden Kontrollkästchen.

ZUSÄTZLICHE MERKMALE FÜR DIE SPAM-FILTERUNG VERWENDEN

Neben den Hauptmerkmalen, auf deren Grundlage die Spam-Filterung von Nachrichten erfolgt (Erstellen von Listen mit erlaubten und verbotenen Absendern, Analyse mit Hilfe von Erkennungsalgorithmen u.a.) können Sie zusätzliche Merkmale festlegen. Auf Basis dieser Merkmale wird einer E-Mail mit einer bestimmten Wahrscheinlichkeitsstufe der Status *Spam* zugewiesen.

Gehen Sie folgendermaßen vor, um bestimmte Zusatzmerkmale für die Spam-Filterung zu verwenden / nicht zu verwenden:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Anti-Spam** aus.
3. Klicken Sie für die ausgewählte Komponente auf die Schaltfläche **Einstellungen**.
4. Klicken Sie im folgenden Fenster auf der Registerkarte **Algorithmus** auf die Schaltfläche **Erweitert**.
5. Aktivieren / deaktivieren Sie im folgenden Fenster **Erweitert** das Kontrollkästchen neben den erforderlichen E-Mail-Merkmalen.

MARKIERUNG ZUM BETREFF EINER NACHRICHT HINZUFÜGEN

Sie können festlegen, dass Nachrichten, die sich bei der Untersuchung als Spam oder potentieller Spam erweisen, im Feld **Betreff** die Markierung **[!! SPAM]** oder **[?? Probable Spam]** erhalten.

Gehen Sie folgendermaßen vor, damit dem Betreff der Nachrichten Markierungen hinzugefügt / nicht hinzugefügt werden:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Anti-Spam** aus.
3. Klicken Sie für die ausgewählte Komponente auf die Schaltfläche **Einstellungen**.
4. Aktivieren / deaktivieren Sie im folgenden Fenster **Erweitert** im Block **Aktionen** die entsprechenden Kontrollkästchen . Sie können den Text der Markierung ändern.

FILTERUNG VON E-MAILS AUF DEM SERVER. MAIL-MANAGER

Sie können eine Liste der E-Mails auf dem Server anzeigen, ohne die Nachrichten auf Ihren Computer herunterzuladen. Dadurch wird Ihnen erlaubt, den Empfang bestimmter Nachrichten abzulehnen, wodurch Sie nicht nur Zeit und Geld bei der Arbeit mit elektronischer Post sparen, sondern auch die Wahrscheinlichkeit des Downloads von Spam und Viren auf Ihren Computer reduzieren können.

Für die Arbeit mit E-Mails auf dem Server dient der **Mail-Manager**. Das Fenster des Mail-Managers wird jedes Mal geöffnet, bevor E-Mails heruntergeladen werden (unter der Bedingung, dass er aktiviert ist).

Das Fenster des Mail-Managers wird nur geöffnet, wenn E-Mails mit dem Protokoll POP3 empfangen werden. Der Mail-Manager wird nicht geöffnet, wenn der POP3-Server die Ansicht von E-Mail-Kopfzeilen nicht unterstützt oder alle auf dem Server vorhandenen E-Mails von Benutzern aus der Liste mit erlaubten Absendern stammen.

Der mittlere Bereich des Manager-Fensters enthält eine Liste der E-Mails auf dem Server. Wählen Sie eine Nachricht aus der Liste, um Details aus ihrer Kopfzeile zu lesen. Die Voransicht von Kopfzeilen kann beispielsweise in folgender Situation von Nutzen sein: Ein Spammer hat auf dem Computer Ihres Kollegen ein Schadprogramm installiert, das unter seinem Namen Spam verschickt und dabei das Adressbuch des Mailprogramms verwendet. Die Wahrscheinlichkeit, dass sich Ihre Adresse im Adressbuch eines Kollegen befindet, ist sehr hoch, was zwangsläufig dazu führt, dass Ihre Mailbox mit Spam überhäuft wird. Es ist unmöglich, in dieser Situation nur aufgrund der Absenderadresse zu ermitteln, ob eine Nachricht von Ihrem Kollegen oder von einem Spammer stammt. Eben deshalb ist es wichtig, die Kopfzeilen der Nachrichten zu berücksichtigen. Es sollte geprüft werden, wann und von wem eine Nachricht abgeschickt wurde. Außerdem sollte die Größe beachtet werden. Verfolgen Sie möglichst auch die Route, die eine E-Mail vom Absender bis zu Ihrem Mailserver zurückgelegt hat. Entsprechende Informationen sind in der Regel im Nachrichten-Header enthalten. Alle entsprechenden Informationen befinden sich in den Kopfzeilen der Nachricht. Das beschriebene Vorgehen hilft Ihnen bei der Entscheidung, ob eine E-Mail wirklich vom Server heruntergeladen oder besser gelöscht werden sollte.

Gehen Sie folgendermaßen vor, um den Mail-Manager zu verwenden:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Anti-Spam** aus.
3. Klicken Sie für die ausgewählte Komponente auf die Schaltfläche **Einstellungen**.

4. Aktivieren Sie im folgenden Fenster auf der Registerkarte **Erweitert** im Block **Eingehende Mails** das Kontrollkästchen **Mail-Manager bei Mailempfang mit POP3-Protokoll öffnen**.

Gehen Sie folgendermaßen vor, um E-Mails mit Hilfe des Mail-Managers vom Server zu löschen:

1. Aktivieren Sie im Fenster des Mail-Managers das der Nachricht entsprechende Kontrollkästchen in der Spalte **Löschen**.

2. Klicken Sie im oberen Bereich des Fensters auf die Schaltfläche **Die markierten löschen**.

Die Nachrichten werden vom Server gelöscht. Dabei erhalten Sie eine Benachrichtigung, die als **[!! SPAM]** markiert und nach den Regeln Ihres Mailprogramms verarbeitet wird.

NACHRICHTEN FÜR MICROSOFT EXCHANGE SERVER VON DER UNTERSUCHUNG AUSSCHLIEßEN

Sie können E-Mails, die im Rahmen eines internen Netzwerks (z.B. Firmenpost) verschickt werden, von der Spam-Untersuchung ausschließen. Beachten Sie, dass dann E-Mails als interne Mail betrachtet werden, wenn als Mail-Client auf allen Netzwerkcomputern das Programm Microsoft Office Outlook benutzt wird und die Mailboxen der Benutzer sich auf einem Exchange-Server oder auf den Servern, die mit X400-Konnektoren verbunden sind, befinden.

In der Grundeinstellung werden Nachrichten für Microsoft Exchange Server nicht von Anti-Spam untersucht.

Gehen Sie folgendermaßen vor, damit Anti-Spam diese Nachrichten analysiert:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.

2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Anti-Spam** aus.

3. Klicken Sie für die ausgewählte Komponente auf die Schaltfläche **Einstellungen**.

4. Deaktivieren Sie im folgenden Fenster auf der Registerkarte **Erweitert** im Block **Ausnahmen** das Kontrollkästchen **E-Mails für Microsoft Exchange Server nicht untersuchen**.

AKTIONEN FÜR UNERWÜNSCHTE E-MAILS

Wenn sich aufgrund einer Untersuchung ergibt, dass eine Nachricht als Spam oder potentieller Spam gilt, sind die weiteren Operationen von Anti-Spam vom Status des Objekts und der ausgewählten Aktion abhängig. Standardmäßig werden E-Mails, die als Spam oder potentieller Spam gelten, modifiziert: Einer Nachricht wird im Feld **Betreff** die Markierung **[!! SPAM]** oder **[?? Probable Spam]** hinzugefügt.

Sie können Zusatzaktionen für Spam und potentiellen Spam festlegen. In den Mailprogrammen Microsoft Office Outlook (s. Abschnitt "Spam-Verarbeitung in Microsoft Office Outlook anpassen" auf S. 119) und Microsoft Outlook Express (Windows Mail) (s. Abschnitt "Spam-Verarbeitung in Microsoft Outlook Express (Windows Mail) anpassen" auf S. 120) sind dafür spezielle Erweiterungsmodule vorgesehen. Für die Mailprogramme The Bat! (s. Abschnitt "Spam-Verarbeitung in The Bat! anpassen" auf S. 121) und Thunderbird (s. Abschnitt "Spam-Verarbeitung in Thunderbird anpassen" auf S. 122) können Sie Filterregeln erstellen.

SIEHE AUCH

Spam-Verarbeitung in Microsoft Office Outlook anpassen 119

Spam-Verarbeitung in Microsoft Outlook Express (Windows Mail) anpassen 120

Spam-Verarbeitung in The Bat! anpassen 121

Spam-Verarbeitung in Thunderbird anpassen 122

SPAM-VERARBEITUNG IN MICROSOFT OFFICE OUTLOOK ANPASSEN

Das Einstellungsfenster für die Spam-Bearbeitung erscheint automatisch, wenn das Mailprogramm nach der Installation von Kaspersky Internet Security zum ersten Mal gestartet wird.

E-Mails, die Anti-Spam als Spam oder potentieller Spam klassifiziert, werden im Feld **Betreff** standardmäßig durch die Markierungen **[!! SPAM]** oder **[?? Probable Spam]** gekennzeichnet.

Sowohl für Spam als auch für potentiellen Spam können Sie folgende Verarbeitungsregeln festlegen:

- **Verschieben in Ordner** – Unerwünschte E-Mails werden in den von Ihnen gewählten Ordner verschoben.
- **Kopieren in Ordner** – Eine Kopie der Nachricht wird angelegt und in den gewählten Ordner verschoben. Die Originalnachricht verbleibt im Ordner **Posteingang**.
- **Löschen** – Unerwünschte E-Mails werden aus der Mailbox des Benutzers gelöscht.
- **Überspringen** – Die Nachricht verbleibt im Ordner **Posteingang**.

Wählen Sie dazu im Block **Spam** oder **Potentieller Spam** den entsprechenden Wert aus der Dropdown-Liste.

Die beim Anti-Spam-Training mit Hilfe eines Mailprogramms (s. Abschnitt "Training mit Hilfe eines Mailprogramms" auf S. 108) markierten E-Mails werden als Spam-Muster an Kaspersky Lab geschickt. Klicken Sie auf den Link **Zusätzliche Aktion, wenn E-Mails manuell als Spam markiert werden**, um im folgenden Fenster einen Modus zum Senden von Spam-Mustern auszuwählen. Klicken Sie auf den Link **Zusätzliche Aktion, wenn E-Mails manuell als Kein Spam markiert werden**, um im folgenden Fenster einen Modus zum Senden von Mustern für "Kein Spam" auszuwählen (Muster, die irrtümlicherweise als Spam eingestuft wurden).

Außerdem können Sie den Algorithmus für die Zusammenarbeit des Programms Microsoft Office Outlook und des Plug-ins von Anti-Spam festlegen:

- **Bei Empfang untersuchen**. Alle Nachrichten, die in der Mailbox des Benutzers eintreffen, werden zuerst entsprechend den für Microsoft Office Outlook festgelegten Regeln bearbeitet. Nach Abschluss dieser Verarbeitung werden die übrigen Nachrichten, die unter keine Regel fallen, zur Verarbeitung an das Erweiterungsmodul von Anti-Spam übergeben. Die Verarbeitung der Nachrichten erfolgt also in einer bestimmten Reihenfolge. Es kann vorkommen, dass diese Reihenfolge unterbrochen wird. Dies kann beispielsweise der Fall sein, wenn gleichzeitig sehr viele Briefe in der Mailbox eintreffen. Dadurch können Informationen über einen Brief, der nach einer Microsoft Office Outlook-Regel bearbeitet wurde, mit dem Status *Spam* im Bericht von Anti-Spam eingetragen wird. Um dies zu vermeiden, wird empfohlen, die Arbeit des Anti-Spam-Plug-ins als Microsoft Office Outlook-Regel zu konfigurieren.
- **Verwenden einer Microsoft Office Outlook-Regel**. In diesem Fall werden die Nachrichten, die in der Benutzermailbox eintreffen, entsprechend der Hierarchie der für das Programm Microsoft Office Outlook erstellten Regeln bearbeitet. Dabei muss eine Regel für die Nachrichtenverarbeitung durch Anti-Spam erstellt werden. Dieser Algorithmus gilt für die Arbeit als optimal, da keine Konflikte zwischen dem Programm Microsoft Office Outlook und dem Anti-Spam-Erweiterungsmodul auftreten. Der Algorithmus besitzt nur einen Nachteil: Eine Spam-Verarbeitungsregel muss manuell über das Programm Microsoft Office Outlook erstellt oder gelöscht werden.

Gehen Sie folgendermaßen vor, um eine Regel zur Spam-Verarbeitung von Nachrichten zu erstellen:

1. Starten Sie das Programm Microsoft Office Outlook und verwenden Sie den Befehl **Extras → Regeln und Benachrichtigungen** im Programmhauptfenster. Die Methode für den Start des Assistenten ist von der Microsoft Office Outlook-Version abhängig, die Sie verwenden. In dieser Hilfe wird das Erstellen einer Regel mit Hilfe von Microsoft Office Outlook 2003 beschrieben.

2. Gehen Sie im Fenster **Regeln und Benachrichtigungen** auf die Registerkarte **Regeln für E-Mails** und klicken Sie auf die Schaltfläche **Neu**. Dadurch wird der Assistent zum Erstellen einer neuen Regel gestartet. Er besteht aus einer Folge von Fenstern / Schritten:

   a. Sie können auswählen, ob zum Erstellen der Regel eine Vorlage benutzt werden soll oder nicht. Wählen Sie die Variante **Regel ohne Vorlage erstellen** und wählen Sie als Prüfungsbedingung **Nachrichten bei Ankunft prüfen** aus. Klicken Sie auf **Weiter**.

   b. Klicken Sie im Fenster zur Auswahl der Bedingungen für die Nachrichtenprüfung auf die Schaltfläche **Weiter**, ohne ein Kontrollkästchen zu aktivieren. Bestätigen Sie in der Bestätigungsanfrage die Anwendung dieser Regel auf alle Nachrichten, die Sie erhalten.

   c. Aktivieren Sie im Fenster zur Auswahl der Aktionen für die Nachrichten in der Aktionsliste das Kontrollkästchen **diese mit einer vordefinierten Aktion bearbeiten**. Klicken Sie im unteren Bereich des Fensters auf den Link **einer vordefinierten Aktion**. Wählen Sie aus der Dropdown-Liste den Wert Kaspersky Anti-Spam und klicken Sie auf **OK**.

   d. Klicken Sie im Fenster zur Auswahl von Ausnahmen auf die Schaltfläche **Weiter**, ohne ein Kontrollkästchen zu aktivieren.

   e. Im Fenster zum Abschluss der Regelerstellung können Sie den Namen der Regel ändern (standardmäßig lautet er Kaspersky Anti-Spam). Überprüfen Sie, ob das Kontrollkästchen **Diese Regel aktivieren** aktiviert ist und klicken Sie auf die Schaltfläche **Fertig**.

3. Die neue Regel wird standardmäßig an erste Stelle zur Regelliste im Fenster **Regeln und Benachrichtigungen** hinzugefügt. Wenn Sie möchten, dass die Regel zuletzt auf eine Nachricht angewandt wird, verschieben Sie sie an das Ende der Liste.

Alle Nachrichten, die in der Mailbox ankommen, werden auf der Grundlage von Regeln bearbeitet. Die Verwendungsreihenfolge der Regeln hängt von der Priorität der einzelnen Regeln ab. Die Regeln werden nacheinander verwendet, wobei mit der obersten Regel begonnen wird und die Priorität der Regeln nach unten sinkt. Sie können die Anwendungspriorität der Regeln erhöhen oder senken.

Wenn Sie nicht möchten, dass eine Nachricht zusätzlich nach einer Anti-Spam-Regel bearbeitet wird, nachdem bereits eine Regel angewandt wurde, muss in den Parametern dieser Regel das Kontrollkästchen **keine weiteren Regeln anwenden** aktiviert werden (s. Schritt 3. zum Erstellen der Regel).

Wenn Sie über Erfahrung beim Erstellen von Bearbeitungsregeln für E-Mail-Nachrichten in Microsoft Office Outlook verfügen, können Sie auf der Basis des oben vorgeschlagenen Algorithmus eine eigene Regel für Anti-Spam erstellen.

Die Parameter für die Bearbeitung von Spam und potentiellen Spam befinden sich in Microsoft Office Outlook auf der speziellen Registerkarte **Anti-Spam** im Menü **Extras →Optionen**.

SPAM-VERARBEITUNG IN MICROSOFT OUTLOOK EXPRESS (WINDOWS MAIL) ANPASSEN

Das Einstellungsfenster für die Spam-Verarbeitung erscheint, wenn das Mailprogramm nach der Installation der Anwendung zum ersten Mal gestartet wird.

E-Mails, die Anti-Spam als Spam oder potentieller Spam klassifiziert, werden im Feld **Betreff** standardmäßig durch die Markierungen **[!! SPAM]** oder **[?? Probable Spam]** gekennzeichnet.

Sowohl für Spam als auch für potentiellen Spam können Sie folgende Verarbeitungsregeln festlegen:

- **Verschieben in Ordner** – Unerwünschte E-Mails werden in den von Ihnen gewählten Mailbox-Ordner verschoben.
- **Kopieren in Ordner** – Eine Kopie der Nachricht wird angelegt und in den gewählten Ordner verschoben. Die Originalnachricht verbleibt im Ordner **Posteingang**.
- **Löschen** – Unerwünschte E-Mails werden aus der Mailbox des Benutzers gelöscht.
- **Überspringen** – Die Nachricht verbleibt im Ordner **Posteingang**.

Um die erforderliche Verarbeitungsregel festzulegen, wählen Sie im Block **Spam** oder **Potentieller Spam** in der Dropdown-Liste den entsprechenden Wert aus.

Die beim Anti-Spam-Training mit Hilfe eines Mailprogramms (s. Abschnitt "Training mit Hilfe eines Mailprogramms" auf S. 108) markierten E-Mails werden als Spam-Muster an Kaspersky Lab geschickt. Klicken Sie auf den Link **Zusätzliche Aktion, wenn E-Mails manuell als Spam markiert werden**, um im folgenden Fenster einen Modus zum Senden von Spam-Mustern auszuwählen. Klicken Sie auf den Link **Zusätzliche Aktion, wenn E-Mails manuell als Kein Spam markiert werden**, um im folgenden Fenster einen Modus zum Senden von Mustern für "Kein Spam" auszuwählen (Muster, die irrtümlicherweise als Spam eingestuft wurden).

Das Einstellungsfenster für die Methoden der Spam-Verarbeitung wird mit der Schaltfläche **Einstellungen** geöffnet, die sich neben den anderen Anti-Spam-Schaltflächen in der Taskleiste befindet : **Spam** und **Kein Spam**.

SPAM-VERARBEITUNG IN THE BAT! ANPASSEN

Die Aktionen für Spam und potentiellen Spam werden im Mailprogramm The Bat! mit den Mitteln des Mailprogramms festgelegt.

➡ *Gehen Sie folgendermaßen vor, um in The Bat! die Spam-Verarbeitungsregeln anzupassen:*

1. Wählen Sie im Menü **Optionen** des Mailprogramms den Punkt **Benutzereinstellungen**.
2. Wählen Sie in der Konfigurationsstruktur den Punkt **Anti-Virus-Plug-Ins**.

Die angezeigten Parameter für den Spam-Schutz gelten für alle auf dem Computer installierten Anti-Spam-Module, die die Arbeit mit The Bat! unterstützen.

Sie müssen eine Score-Stufe festlegen und die Aktion angeben, die auf Nachrichten angewandt werden soll, denen ein bestimmter Score zugewiesen wurde (im Fall von Anti-Spam ist das die Wahrscheinlichkeit, dass eine E-Mail als Spam gilt):

- Nachricht mit einem Score, der den Grenzwert überschreitet, löschen.
- Nachricht mit einem bestimmten Score in einen speziellen Ordner für Spam-Nachrichten verschieben.
- Spam-Nachrichten, die mit einer speziellen Kopfzeile markiert sind, in den Spam-Ordner verschieben.
- Spam-Nachrichten im Ordner **Eingang** belassen.

Aufgrund der Bearbeitung von E-Mail-Nachrichten durch Kaspersky Internet Security wird der Nachricht auf der Basis eines Faktors, den Sie festlegen können, der Status Spam oder potentieller Spam zugewiesen. Im Mailprogramm The Bat! ist ein entsprechender Score-Algorithmus für Nachrichten intrigiert, und ebenfalls auf dem Spam-Faktor basiert. Um Differenzen zwischen den Spam-Faktoren in Kaspersky Internet Security und in The Bat! zu vermeiden, werden alle von Anti-Spam geprüften Nachrichten dem Rating angepasst, das dem Status der Nachricht entspricht: erwünschte E-Mails – 0%, potentieller Spam – 50%, Spam – 100%. Dadurch stimmt der Score der Nachricht im Mailprogramm The Bat! nicht mit dem in Anti-Spam festgelegten Faktor der Nachricht überein, sondern mit dem Faktor des entsprechenden Status.

Einzelheiten über den Spam-Score und die Verarbeitungsregeln s. Dokumentation zum Mailprogramm The Bat!

SPAM-VERARBEITUNG IN THUNDERBIRD ANPASSEN

E-Mails, die Anti-Spam als Spam oder potentieller Spam klassifiziert, werden im Feld **Betreff** standardmäßig durch die Markierungen **[!! SPAM]** oder **[?? Probable Spam]** gekennzeichnet. In Thunderbird werden solche Nachrichten mit Hilfe von Regeln im Menü **Extras** → **Filter** behandelt (Details über die Arbeit mit dem Mail-Client s. Hilfe zu Mozilla Thunderbird).

Das Anti-Spam-Erweiterungsmodul für Thunderbird erlaubt es, ein Training mit E-Mails vorzunehmen, die mit diesem Mail-Client empfangen und gesendet wurden. Außerdem kann die E-Mail-Korrespondenz auf Spam untersucht werden. Das Modul wird in Thunderbird integriert und leitet E-Mails zur Untersuchung an die Komponente Anti-Spam um. Dazu dient der Menübefehl **Extras** → **Junk-Filter auf Ordner anwenden**. Die Nachrichtenuntersuchung wird also nicht von Thunderbird, sondern von Kaspersky Internet Security ausgeführt. Dabei bleibt die Funktionalität von Thunderbird unverändert.

Der Status des Anti-Spam-Erweiterungsmoduls wird in Form eines Symbols in der Statuszeile von Thunderbird angezeigt. Das graue Symbol bedeutet, dass bei der Arbeit des Plug-ins ein Problem vorliegt oder dass die Komponente Anti-Spam (auf S. 103) deaktiviert wurde. Durch Doppelklick auf das Symbol wird das Konfigurationsfenster von Kaspersky Internet Security geöffnet. Um zu den Einstellungen für **Anti-Spam** zu gelangen, klicken Sie im Block **Anti-Spam** auf die Schaltfläche **Einstellungen**.

STANDARDPARAMETER FÜR ANTI-SPAM WIEDERHERSTELLEN

Während Sie die Arbeit von Anti-Spam anpassen, können Sie jederzeit zu den empfohlenen Einstellungen zurückkehren. Diese gelten als optimal, werden von den Kaspersky-Lab-Spezialisten empfohlen und sind in der Sicherheitsstufe **Empfohlen** zusammengefasst.

Gehen Sie folgendermaßen vor, um die standardmäßigen Einstellungen für den Schutz vor unerwünschten E-Mails wiederherzustellen,

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Anti-Spam** aus.
3. Klicken Sie für die ausgewählte Komponente im Block **Sicherheitsstufe** auf die Schaltfläche **Standard**.

ANTI-BANNER

Anti-Banner blockiert Werbung, die auf speziellen Bannern platziert ist, die in das Interface von auf Ihrem Computer installierten Programmen integriert sind oder sich im Internet befinden.

Bannerwerbung enthält nicht nur unnütze Informationen, sondern lenkt Sie auch von der Arbeit ab und erhöht das Volumen des Datenverkehrs. Anti-Banner blockiert die momentan meist verbreiteten Banner, deren Masken im Lieferumfang von Kaspersky Internet Security enthalten sind. Sie können das Blockieren von Bannern ausschalten oder eigene Listen mit erlaubten und verbotenen Bannern erstellen.

Eine Liste mit Masken der häufigsten Werbebanner wurde von den Kaspersky-Lab-Spezialisten auf der Basis spezieller Untersuchungen erstellt und in den Lieferumfang Kaspersky Internet Security aufgenommen. Die Werbebanner, die einer Maske dieser Liste entsprechen, werden vom Anti-Banner gesperrt, falls das Blockieren von Bannern nicht deaktiviert wurde. Zum Sperren von Bannern, deren Adressenmasken nicht in der Standardliste enthalten sind, wird eine heuristische Analyse verwendet (s. Abschnitt "Heuristische Analyse verwenden" auf S. 123).

Außerdem können Sie eine weiße (s. Abschnitt "Liste der erlaubten Banneradressen erstellen" auf S. 124) und schwarze (s. Abschnitt "Liste der verbotenen Banneradressen erstellen" auf S. 125) Bannerliste anlegen, auf deren Grundlage der Empfang von Bannern erlaubt bzw. verboten wird.

Anti-Banner ist nach der Installation von Kaspersky Internet Security deaktiviert.

➧ *Gehen Sie folgendermaßen vor, um die Funktionsparameter von Anti-Banner anzupassen:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Anti-Banner** aus.
3. Passen Sie die Parameter der ausgewählten Komponente entsprechend an.

IN DIESEM ABSCHNITT

Heuristische Analyse verwenden 123

Erweiterte Einstellungen für die Komponente 124

Liste der erlaubten Banneradressen erstellen 124

Liste der verbotenen Banneradressen erstellen 125

Bannerlisten exportieren / importieren 125

HEURISTISCHE ANALYSE VERWENDEN

Banner, deren Adressen nicht in der Standardliste enthalten sind, können mit Hilfe der heuristischen Analyse analysiert werden. Wenn sie verwendet wird, analysiert Kaspersky Internet Security heruntergeladene Grafiken auf das Vorhandensein charakteristischer Bannermerkmale. Aufgrund solcher Analyse können Grafiken als Banner identifiziert und blockiert werden.

➧ *Gehen Sie folgendermaßen vor, um die heuristische Analyse zu verwenden:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Anti-Banner** aus.

3. Aktivieren Sie für die ausgewählte Komponente im Block **Untersuchung** das Kontrollkästchen **Heuristische Analyse verwenden**.

ERWEITERTE EINSTELLUNGEN FÜR DIE KOMPONENTE

Eine Liste mit Masken der häufigsten Werbebanner wurde von den Kaspersky-Lab-Spezialisten auf der Basis spezieller Untersuchungen erstellt und in den Lieferumfang Kaspersky Internet Security aufgenommen. Die Werbebanner, die einer Maske dieser Liste entsprechen, werden vom Anti-Banner gesperrt, falls das Blockieren von Bannern nicht deaktiviert wurde.

Beim Erstellen von Listen mit erlaubten / verbotenen Bannern können IP-Adressen oder deren symbolische Namen (URL-Adresse) angegeben werden. Um Doppelnennungen zu vermeiden, können Sie eine Zusatzfunktion aktivieren, mit der eingegebene IP-Adressen in Domänennamen umgewandelt werden können und umgekehrt.

- *Gehen Sie folgendermaßen vor, um die Verwendung der im Lieferumfang von Kaspersky Internet Security enthaltenen Bannerliste zu deaktivieren:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Anti-Banner** aus.
3. Deaktivieren Sie für die ausgewählte Komponente im Block **Untersuchung** das Kontrollkästchen **Standardliste für Banner verwenden**.

- *Gehen Sie folgendermaßen vor, um die Funktion zur Umwandlung von eingegebenen IP-Adressen in Domänennamen (Domänennamen in IP-Adressen) zu verwenden:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Anti-Banner** aus.
3. Aktivieren Sie für die ausgewählte Komponente im Block **Untersuchung** das Kontrollkästchen **IP-Adressen in Domänennamen umwandeln**.

LISTE DER ERLAUBTEN BANNERADRESSEN ERSTELLEN

Die weiße Bannerliste wird vom Benutzer bei der Arbeit mit Kaspersky Internet Security erstellt, wenn es erforderlich ist, bestimmte Banner nicht zu blockieren. Diese Liste enthält die für den Empfang zugelassenen Banner.

- *Gehen Sie folgendermaßen vor, um der weißen Liste eine neue Maske hinzuzufügen:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Anti-Banner** aus.
3. Aktivieren Sie für die ausgewählte Komponente im Block **Erweitert** das Kontrollkästchen **Weiße Adressenliste verwenden** und klicken Sie auf die Schaltfläche **Einstellungen**.
4. Klicken Sie im folgenden Fenster **Weiße Liste** auf den Link **Hinzufügen**.
5. Geben Sie im folgenden Fenster **Adressenmaske (URL)** die Maske eines erlaubten Banners an. Damit eine bestimmte Maske nicht verwendet wird, ist es ausreichend, das entsprechende Kontrollkästchen zu deaktivieren.

LISTE DER VERBOTENEN BANNERADRESSEN ERSTELLEN

Sie können eine Liste mit verbotenen Banneradressen anlegen, die gegebenenfalls von Anti-Banner blockiert werden sollen.

Gehen Sie folgendermaßen vor, um der schwarzen Liste eine neue Maske hinzuzufügen:

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Anti-Banner** aus.
3. Aktivieren Sie für die ausgewählte Komponente im Block **Erweitert** das Kontrollkästchen **Schwarze Adressenliste verwenden** und klicken Sie auf die Schaltfläche **Einstellungen**.
4. Klicken Sie im folgenden Fenster **Schwarze Liste** auf den Link **Hinzufügen**.
5. Geben Sie im folgenden Fenster **Adressenmaske (URL)** die Maske eines verbotenen Banners an. Damit eine bestimmte Maske nicht verwendet wird, ist es ausreichend, das entsprechende Kontrollkästchen zu deaktivieren.

BANNERLISTEN EXPORTIEREN / IMPORTIEREN

Sie können vorhandene Listen mit erlaubten bzw. verbotenen Bannern von einem Computer auf einen anderen kopieren. Beim Export einer Liste können Sie auswählen, ob nur die gewählten Listenelemente oder die gesamte Liste kopiert werden soll. Beim Import können der Liste neue Adressen hinzugefügt oder die vorhandene Liste durch eine importierte ersetzt werden.

Gehen Sie folgendermaßen vor, um vorhandene Listen mit erlaubten / verbotenen Bannern zu kopieren:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Anti-Banner** aus.
3. Klicken Sie für die ausgewählte Komponente im Block **Erweitert** für die Liste, die kopiert werden soll, auf die Schaltfläche **Einstellungen**.
4. Verwenden Sie im folgenden Fenster **Weiße Liste** (oder im Fenster **Schwarze Liste**) die Links **Import** oder **Export**.

KINDERSICHERUNG

Die Programmkomponente *Kindersicherung* kontrolliert den Zugriff von Computerbenutzern auf Webressourcen. Die Hauptaufgabe der Kindersicherung besteht darin, den Zugriff auf folgende Ressourcen zu beschränken:

- Webseiten, die für Erwachsene bestimmt sind, oder Webseiten, die Themen wie Pornografie, Waffen, Drogen betreffen oder Grausamkeit, Gewalt usw. provozieren.
- Webseiten, die Zeitverlust (Chats, Spielressourcen) oder Geldverlust (Internet-Shops, Auktionen) verursachen können.

Solche Webseiten enthalten häufig mehrere Schadprogramme. Außerdem verursacht der Download von Daten aus Ressourcen wie beispielsweise Spielseiten eine bedeutende Erhöhung des Internet-Datenverkehrs.

Der Zugriff eines Benutzers auf Webressourcen wird beschränkt, indem ihm eines der drei vorgegebenen Profile (s. S. 128) für die Arbeit im Internet zugeordnet wird. Für jedes Profil können Beschränkungen im Hinblick auf die Anzeige (s. S. 130) und Verwendungszeit von Webressourcen (s. S. 134) festgelegt werden.

In der Grundeinstellung gilt für alle Benutzer das Profil **Kind**, das die maximalen Beschränkungen besitzt. Ein Profil kann mit Benutzerkonten von Microsoft Windows verbunden werden. In diesem Fall erhält der Benutzer in Abhängigkeit von den Parametern seines Profils Zugriff auf Webressourcen.

Der Zugriff auf die Profile **Erwachsener** und **Jugendlicher** sollte durch ein Kennwort geschützt werden. Der Wechsel zu einem Profil (s. S. 128), das kennwortgeschützt ist, ist erst nach der Angabe des Kennworts möglich.

Jedes Profil reguliert den Zugriff auf Webseiten auf einem der vordefinierten Beschränkungsniveaus (s. S. 129). Eine Beschränkungsstufe ist eine Auswahl von Parametern, die den Zugriff auf Internetressourcen regulieren.

Es wird empfohlen, den Kennwortschutz für Kaspersky Internet Security anzupassen (s. Abschnitt "Selbstschutz für Kaspersky Internet Security" auf S. 170), um ein unerlaubtes Ausschalten der Komponente zu verhindern.

Die Kindersicherung ist nach der Installation von Kaspersky Internet Security deaktiviert.

Gehen Sie folgendermaßen vor, um die Funktionsparameter der Kindersicherung zu ändern:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Kindersicherung** aus.
3. Klicken Sie für die ausgewählte Komponente auf die Schaltfläche **Einstellungen**.
4. Passen Sie die Parameter der Komponente entsprechend an.

IN DIESEM ABSCHNITT

Algorithmus für die Arbeit der Komponente 127

Arbeit mit Profilen 128

Profile wechseln 128

Beschränkungsniveau ändern 129

Beschränkungen für die Anzeige von Webressourcen 130

Liste mit erlaubten Webadressen erstellen 130

Liste mit verbotenen Webadressen erstellen 132

Liste mit Webadressen exportieren / importieren 132

Kategorien für verbotene Webadressen auswählen 133

Heuristische Analyse verwenden 134

Aktion bei einem Zugriffsversuch auf verbotene Webadressen auswählen 134

Zeitbeschränkung für den Zugriff 134

ALGORITHMUS FÜR DIE ARBEIT DER KOMPONENTE

Der allgemeine Funktionsalgorithmus der Komponente **Kindersicherung** lässt sich folgendermaßen beschreiben.

1. Bei der Authentifizierung des Benutzers nach dem Hochfahren des Systems wird das Profil geladen, das diesem Benutzer entspricht.

2. Wenn ein Benutzer versucht, auf eine Webseite zuzugreifen, führt die Kindersicherung folgende Aktionen aus:

   - Überprüfung, ob eine Zeitbeschränkung vorliegt (s. S. 134).

   - Überprüfung, ob die URL der angeforderten Seite mit einem Element der Liste mit erlaubten Adressen übereinstimmt, wenn der Modus für den ausschließlichen Zugriff auf bestimmte Webseiten gewählt wurde.

   - Wenn der Modus mit Beschränkungen gewählt wurde, führt die Komponente folgende Aktionen aus:

     - Überprüfung, ob die URL der angeforderten Seite mit einem Element der Listen mit erlaubten und verbotenen Adressen übereinstimmt.

     - Analyse des Inhalts der Webseite auf die Zugehörigkeit der Seite zu einer verbotenen Kategorie.

Wird mindestens eine dieser Bedingungen nicht erfüllt, so wird der Zugriff auf die Seite gesperrt. Andernfalls wird die Webseite im Browserfenster geladen.

Wenn in Ihrem Netzwerk ein Proxyserver verwendet wird, der einen nicht standardmäßigen Port benutzt, ist es erforderlich, diesen Port zur Liste der kontrollierten Ports (s. Abschnitt "Liste der zu kontrollierenden Ports erstellen" auf S. 178) hinzuzufügen. Andernfalls kann es sein, dass die Kindersicherung fehlerhaft arbeitet und verbotene Webseiten erlaubt.

Wenn eine angeforderte Webseite aufgrund der Untersuchung als verboten eingestuft wird, wird der Zugriff darauf blockiert. Andernfalls wird die Webseite im Browserfenster geladen.

ARBEIT MIT PROFILEN

Ein Profil ist eine Auswahl von Regeln, die den Zugriff eines Benutzers auf bestimmte Internetressourcen regulieren. Folgende Profile stehen zur Auswahl: **Kind** (wird standardmäßig verwendet), **Jugendlicher** oder **Erwachsener**.

Für jedes dieser Profile wurde eine optimale Kombination von Regeln erarbeitet, die Alter, Erfahrung und andere Merkmale der jeweiligen Gruppe berücksichtigen Das Profil **Kind** besitzt die meisten Beschränkungen, wogegen das Profil **Erwachsener** keine Beschränkungen aufweist. Es können keine eigenen Profile erstellt werden und die vordefinierten Profile können nicht gelöscht werden. Allerdings können die Parameter der Profile **Kind** und **Jugendlicher** nach eigenem Ermessen angepasst werden.

Für die Profile **Erwachsener** und **Jugendlicher** sollte unbedingt ein Kennwort festgelegt werden. Das Kennwort wird beim Wechseln von Profilen (s. S. 128) abgefragt.

Gehen Sie folgendermaßen vor, um die Profile Jugendlicher und Erwachsener zu verwenden:

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Kindersicherung** aus.
3. Klicken Sie für die ausgewählte Komponente auf die Schaltfläche **Einstellungen**.
4. Aktivieren Sie im folgenden Fenster auf der Registerkarte **Jugendlicher** oder auf der Registerkarte **Erwachsener** das Kontrollkästchen **Profil verwenden** und legen Sie im entsprechenden Feld ein Kennwort fest.

Gehen Sie folgendermaßen vor, um ein Profil mit einem Benutzerkonto von Microsoft Windows zu verbinden:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Kindersicherung** aus.
3. Klicken Sie für die ausgewählte Komponente auf die Schaltfläche **Einstellungen**.
4. Klicken Sie im folgenden Fenster auf der Registerkarte **Jugendlicher** oder auf der Registerkarte **Erwachsener** im Block **Liste der Benutzer** auf den Link **Hinzufügen**.
5. Das folgende Fenster **Benutzer** enthält eine Liste der lokalen Benutzerkonten. Wählen Sie das erforderliche Konto in der Liste aus und klicken Sie auf **OK**.

   Wenn ein Benutzerkonto, das nicht in der Liste enthalten ist, hinzugefügt werden soll, verwenden Sie dazu die Standardmittel von Microsoft Windows. Klicken Sie dazu auf die Schaltfläche **Suchen** und geben Sie im Standardfenster von Microsoft Windows das erforderliche Konto an (Details s. Hilfe des Betriebssystems).

   Damit ein Profil nicht auf ein Benutzerkonto angewandt wird, markieren Sie diesen Benutzer im Block **Liste der Benutzer** und klicken Sie auf den Link **Löschen**.

PROFILE WECHSELN

Das momentan aktive Profil kann gewechselt werden. Dies kann erforderlich sein, wenn das aktive Profil Beschränkungen für den Zugriff auf Internetressourcen aufweist und Sie bei der Arbeit im Internet behindert.

Profile können aus dem Kontextmenü (см. Abschnitt "Kontextmenü" auf S. 42) des Programms umgeschaltet werden.

Das Umschalten von Profilen wird durch ein Kennwort kontrolliert. Um zum Profil **Kind** zu wechseln, wird kein Kennwort benötigt.

Gehen Sie folgendermaßen vor, um das Benutzerprofil vom Kontextmenü aus zu wechseln:

1. Klicken Sie im Infobereich der Taskleiste mit der rechten Maustaste auf das Programmsymbol.
2. Wählen Sie im Kontextmenü den Punkt **Kindersicherung** aus.
3. Wählen Sie im Kontextmenü das gewünschte Profil aus.
4. Geben Sie im folgenden Fenster **Profil wechseln** das Kennwort an. Beim Wechsel in das Profil **Kind** fehlt dieses Fenster.

Gehen Sie folgendermaßen vor, um ein Kennwort für ein Benutzerprofil zu wechseln:

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Kindersicherung** aus.
3. Klicken Sie für die ausgewählte Komponente auf die Schaltfläche **Einstellungen**.
4. Geben Sie im folgenden Fenster auf der Registerkarte **Jugendlicher** oder auf der Registerkarte **Erwachsener** im entsprechenden Feld das Kennwort ein.

BESCHRÄNKUNGSNIVEAU ÄNDERN

Die Kindersicherung bietet die Kontrolle über den Zugriff von Computerbenutzern auf Internetressourcen mit einer der vordefinierten Stufe.

Wenn keine der vordefinierten Beschränkungsstufen vollständig Ihren Anforderungen entspricht, können Sie die Parameter zusätzlich anpassen. Wählen Sie dazu die Stufe, die Ihren Anforderungen am nächsten kommt, als Ausgangsstufe und ändern Sie die Parameter entsprechend.

Für das Profil **Erwachsener** gibt es keine Beschränkungsstufen.

Gehen Sie folgendermaßen vor, um die Beschränkungsstufe zu ändern:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Kindersicherung** aus.
3. Klicken Sie für die ausgewählte Komponente auf die Schaltfläche **Einstellungen**.
4. Stellen Sie im folgenden Fenster auf der Registerkarte des erforderlichen Profils (**Kind** oder **Jugendlicher**) mit Hilfe des Schiebereglers im Block **Beschränkungsstufe** die entsprechende Beschränkungsstufe ein.

Gehen Sie folgendermaßen vor, um die Parameter einer Beschränkungsstufe anzupassen:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Kindersicherung** aus.
3. Klicken Sie für die ausgewählte Komponente auf die Schaltfläche **Einstellungen**.
4. Stellen Sie im folgenden Fenster auf der Registerkarte des erforderlichen Profils (**Kind** oder **Jugendlicher**) mit Hilfe des Schiebereglers im Block **Beschränkungsstufe** die entsprechende Beschränkungsstufe ein und klicken Sie auf die Schaltfläche **Einstellungen**.

5. Das folgende Fenster erlaubt es, die Anzeige von Webressourcen (s. S. 130) und die Dauer des Internetzugriffs (s. S. 134) zu beschränken, die Genauigkeit der heuristischen Analyse festzulegen (s. S. 134) und eine Liste der Kategorien für verbotene Webadressen anlegen (s. S. 133). Dadurch wird eine vierte Beschränkungsstufe mit der Bezeichnung **Benutzerdefiniert** erstellt, die die von Ihnen definierten Schutzparameter enthält. Klicken Sie im Block **Beschränkungsstufe** auf die Schaltfläche **Standard**, um zu den standardmäßigen Beschränkungsparametern zurückzukehren.

BESCHRÄNKUNGEN FÜR DIE ANZEIGE VON WEBRESSOURCEN

Für die Profile **Kind** und **Jugendlicher** kann die Anzeige bestimmter Webseiten beschränkt werden. Die Kindersicherung bietet zwei Methoden, um den Zugriff auf Internetressourcen zu beschränken:

- Blockieren des Zugriffs auf alle Internetressourcen unter Ausnahme festgelegter erlaubter Ressourcen. Solche Beschränkungen gelten, wenn der Modus gewählt wurde, in dem nur bestimmte Webadressen für den Zugriff zugelassen sind. In diesem Modus erfolgt die Konfiguration durch das Erstellen der Liste mit erlaubten Adressen (s. S. 130).

- Blockieren des Zugriffs auf Internetressourcen nach einer Auswahl von Parametern. Dabei ist der Modus mit Beschränkungen aktiv. Eine Entscheidung darüber, ob der Zugriff auf eine bestimmte Webadresse erlaubt oder verboten wird, erfolgt aufgrund bestimmter Bedingungen:

  - Übereinstimmung einer angeforderten Webseite mit Elementen der Listen für erlaubte (s. S. 130) oder verbotene (s. S. 132) Adressen.

  - Zugehörigkeit einer Webseite zu einer verbotenen Kategorie.

➡ *Gehen Sie folgendermaßen vor, um für das Profil Kind oder Jugendlicher einen Beschränkungsmodus der Kindersicherung auszuwählen:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.

2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Kindersicherung** aus.

3. Klicken Sie für die ausgewählte Komponente auf die Schaltfläche **Einstellungen**.

4. Klicken Sie auf der Registerkarte des Profils, das Sie anpassen möchten, auf die Schaltfläche **Einstellungen**.

5. Wählen Sie im folgenden Fenster **Profil anpassen** auf der Registerkarte **Beschränkungen** eine Variante aus:

   - **Nur erlaubte Webadressen zur Anzeige zulassen** – um den Modus auszuwählen, in dem nur der Zugriff auf bestimmte Seiten erlaubt wird.

   - **Beschränkungen festlegen** – um den Modus mit Beschränkungen auszuwählen.

LISTE MIT ERLAUBTEN WEBADRESSEN ERSTELLEN

Für die Profile **Kind** und **Jugendlicher** können Sie den Zugriff auf bestimmte Webressourcen erlauben. Dazu werden die Adressen der betreffenden Webressourcen zur Liste der erlaubten Webadressen hinzugefügt.

Wenn der Modus, in dem nur bestimmte Webadressen für den Zugriff zugelassen sind, gewählt wurde (Option **Nur erlaubte Webadressen zur Anzeige zulassen**), wird der Zugriff auf alle Seiten, die nicht auf der Liste der erlaubten Adressen stehen, blockiert.

Wenn der Modus mit Beschränkungen gewählt wurde (Option **Beschränkungen festlegen**), kann der Zugriff auf Webressourcen auf Basis der Zugehörigkeit zu bestimmten Kategorien beschränkt werden. Außerdem kann der Zugriff

auf bestimmte Webressourcen explizit verboten werden. Dazu werden die Adressen solcher Internetressourcen zur Liste der verbotenen Adressen hinzugefügt.

Es kann vorkommen, dass eine Ressource, die der Liste für erlaubte Webadressen hinzugefügt wurde, einer Kategorie der verbotenen Webadressen angehört (s. S. 133). In diesem Fall besteht auch dann Zugriff auf diese Ressource, wenn die Filterung von Webseiten nach der entsprechenden Kategorie aktiviert wurde.

Beispiel: Sie möchten verhindern, dass Ihr Kind Webseiten besucht, die für Erwachsene gedacht sind und zu Geld- und Zeitverlust führen können. Gleichzeitig soll das Kind aber E-Mails von Ihnen empfangen können.

Wählen Sie das Profil **Kind**. Als Basis kann die vordefinierte Beschränkungsstufe **Empfohlen** dienen, die folgendermaßen angepasst wird: Chats und Internet-Mail werden verboten, und der externe Maildienst, bei dem Ihr Kind eine Mailbox besitzt, wird der Liste für erlaubte Webadressen hinzugefügt. Mit diesen Einstellungen kann Ihr Kind nur auf diesen Maildienst zugreifen.

Gehen Sie folgendermaßen vor, um der Liste für erlaubte Adressen im Modus, in dem nur bestimmte Webadressen zugelassen sind, eine neue Adresse oder Maske hinzuzufügen:

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Kindersicherung** aus.
3. Klicken Sie für die ausgewählte Komponente auf die Schaltfläche **Einstellungen**.
4. Klicken Sie auf der Registerkarte des Profils, das Sie anpassen möchten, auf die Schaltfläche **Einstellungen**.
5. Klicken Sie im folgenden Fenster **Profil anpassen** auf der Registerkarte **Beschränkungen** auf die Schaltfläche **Liste**.
6. Klicken Sie im folgenden Fenster **Liste der erlaubten Adressen** auf den Link **Hinzufügen**.
7. Geben Sie im folgenden Fenster **Adressenmaske (URL)** eine Adresse oder Maske an.

   Wenn Sie eine Adresse oder eine Maske aus der Liste ausschließen möchten, ohne sie zu löschen, deaktivieren Sie in der Liste das entsprechende Kontrollkästchen.

Gehen Sie folgendermaßen vor, um der Liste für erlaubte Adressen im Modus, in dem Beschränkungen gelten, eine neue Adresse oder Maske hinzuzufügen:

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Kindersicherung** aus.
3. Klicken Sie für die ausgewählte Komponente auf die Schaltfläche **Einstellungen**.
4. Klicken Sie auf der Registerkarte des Profils, das Sie anpassen möchten, auf die Schaltfläche **Einstellungen**.
5. Klicken Sie im folgenden Fenster **Profil anpassen** auf der Registerkarte **Beschränkungen** auf die Schaltfläche **Ausnahmen**.
6. Klicken Sie im folgenden Fenster **Liste der erlaubten Adressen** auf den Link **Hinzufügen**.
7. Geben Sie im folgenden Fenster **Adressenmaske (URL)** eine Adresse oder Maske an.

   Wenn Sie eine Adresse oder eine Maske aus der Liste ausschließen möchten, ohne sie zu löschen, deaktivieren Sie in der Liste das entsprechende Kontrollkästchen.

LISTE MIT VERBOTENEN WEBADRESSEN ERSTELLEN

Im Modus mit Beschränkungen (Option **Festgelegte Beschränkungen verwenden**) beschränkt die Kindersicherung den Zugriff auf Webressourcen, wobei die Zugehörigkeit von Seiten zu bestimmten Kategorien zugrunde gelegt wird (s. Abschnitt "Kategorien für verbotene Webadressen auswählen" auf S. 133). Der Zugriff auf konkrete Webressourcen kann explizit verboten werden. Dazu werden diese Adressen zur Liste der verbotenen Webadressen hinzugefügt.

Gehen Sie folgendermaßen vor, um der Liste der verbotenen Adressen eine neue Adresse oder Maske hinzuzufügen:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Kindersicherung** aus.
3. Klicken Sie für die ausgewählte Komponente auf die Schaltfläche **Einstellungen**.
4. Klicken Sie auf der Registerkarte des Profils, das Sie anpassen möchten, auf die Schaltfläche **Einstellungen**.
5. Klicken Sie im folgenden Fenster **Profil anpassen** auf der Registerkarte **Beschränkungen** auf die Schaltfläche **Liste**.
6. Klicken Sie im folgenden Fenster **Liste der verbotenen Webadressen** auf den Link **Hinzufügen**.
7. Geben Sie im folgenden Fenster **Adressenmaske (URL)** eine Adresse oder Maske an.

   Wenn Sie eine Adresse oder eine Maske aus der Liste ausschließen möchten, ohne sie zu löschen, deaktivieren Sie in der Liste das entsprechende Kontrollkästchen.

LISTE MIT WEBADRESSEN EXPORTIEREN / IMPORTIEREN

Wenn Sie bereits eine Liste mit erlaubten oder verbotenen Webadressen angelegt haben, kann die Liste in einer separaten Datei gespeichert werden. Anschließend kann die Liste aus dieser Datei importiert werden, um die vorhandene Liste zu verwenden. Die Möglichkeit zum Export / Import einer Liste ist beispielsweise vorteilhaft, wenn Sie für die Profile **Kind** und **Jugendlicher** einheitliche Parameter festlegen möchten.

Die Möglichkeit zum Export / Import einer Liste steht nur im Modus mit Beschränkungen zur Verfügung (Variante **Beschränkungen festlegen**).

Gehen Sie folgendermaßen vor, um eine Liste mit Webadressen in einer Datei zu speichern:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Kindersicherung** aus.
3. Klicken Sie für die ausgewählte Komponente auf die Schaltfläche **Einstellungen**.
4. Klicken Sie auf der Registerkarte des Profils, das Sie anpassen möchten, auf die Schaltfläche **Einstellungen**.
5. Öffnen Sie im folgenden Fenster **Profil anpassen** auf der Registerkarte **Beschränkungen** die erforderliche Liste:
   - Liste der erlaubten Webadressen im Modus mit Beschränkungen – mit Hilfe der Schaltfläche **Ausnahmen**.
   - Liste der verbotenen Webadressen im Modus mit Beschränkungen – mit Hilfe der Schaltfläche **Liste**.
6. Klicken Sie im folgenden Fenster mit der Liste der Webadressen auf den Link **Export**.

7. Geben Sie im folgenden Fenster **Speichern unter** an, unter welchem Pfad und Namen die Datei gespeichert werden soll.

Gehen Sie folgendermaßen vor, um eine Liste mit Webadressen aus einer Datei zu laden:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Kindersicherung** aus.
3. Klicken Sie für die ausgewählte Komponente auf die Schaltfläche **Einstellungen**.
4. Klicken Sie auf der Registerkarte des Profils, das Sie anpassen möchten, auf die Schaltfläche **Einstellungen**.
5. Öffnen Sie im folgenden Fenster **Profil anpassen** auf der Registerkarte **Beschränkungen** die erforderliche Liste:
   - Liste der erlaubten Webadressen im Modus mit Beschränkungen – mit Hilfe der Schaltfläche **Ausnahmen**.
   - Liste der verbotenen Webadressen im Modus mit Beschränkungen – mit Hilfe der Schaltfläche **Liste**.
6. Klicken Sie im folgenden Fenster mit der Liste der Webadressen auf den Link **Import**.
7. Geben Sie im folgenden Fenster **Datei öffnen** den Pfad der Datei an.

KATEGORIEN FÜR VERBOTENE WEBADRESSEN AUSWÄHLEN

Die Kindersicherung analysiert den Inhalt von Webseiten nach Schlüsselwörtern, die bestimmten Themenkategorien angehören. Wenn die Anzahl der Wörter einer unerwünschten Kategorie den zulässigen Grenzwert überschreitet, wird der Zugriff auf die Ressource gesperrt. Der Zugriff auf Webadressen kann nach bestimmten Kategorien beschränkt werden, wenn für das Profil der Modus mit Beschränkungen (s. S. 130) gewählt wurde.

Die Datenbank der Schlüsselwörter gehört zum Lieferumfang von Kaspersky Internet Security und wird gemeinsam mit den Datenbanken und Programm-Modulen aktualisiert.

Die Liste der verbotenen Kategorien ist auf eine standardmäßige Liste beschränkt. Es ist nicht möglich, eigene Verbotskategorien anzulegen.

Gehen Sie folgendermaßen vor, um für das Profil Kind oder Jugendlicher die Kategorien der verbotenen Webseiten auszuwählen:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Kindersicherung** aus.
3. Klicken Sie für die ausgewählte Komponente auf die Schaltfläche **Einstellungen**.
4. Klicken Sie auf der Registerkarte des Profils, das Sie anpassen möchten, auf die Schaltfläche **Einstellungen**.
5. Aktivieren Sie im folgenden Fenster **Profil anpassen** auf der Registerkarte **Beschränkungen** dass Kontrollkästchen **Webadressen nach Kategorien blockieren**.
6. Aktivieren Sie dazu die Kontrollkästchen für die entsprechenden Kategorien.

HEURISTISCHE ANALYSE VERWENDEN

In der Grundeinstellung wird eine Datenbank mit Schlüsselwörtern eingesetzt, um zu prüfen, ob Webressourcen verbotenen Kategorien angehören. Zur weiteren Untersuchung von Ressourcen, für die diese Datenbanken keine Ergebnisse erbringen, wird die heuristische Analyse verwendet. Dieser Mechanismus ist sehr effektiv und führt nur selten zu einem Fehlalarm.

Zusätzlich kann das Genauigkeitsniveau der Analyse festlegt werden. Dadurch wird das Verhältnis zwischen Auslastungsniveau der Betriebssystemressourcen, Ausführlichkeit der Suche und Untersuchungsdauer reguliert. Je höher das für die Untersuchung gewählte Niveau, desto mehr Systemressourcen sind dafür erforderlich und desto mehr Zeit wird beansprucht.

Bei Einsatz der tiefen Analysestufe sind Fehlalarme möglich.

Gehen Sie folgendermaßen vor, um die heuristische Analyse zu verwenden und das Genauigkeitsniveau der Analyse festzulegen:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Kindersicherung** aus.
3. Klicken Sie für die ausgewählte Komponente auf die Schaltfläche **Einstellungen**.
4. Klicken Sie auf der Registerkarte des Profils (**Kind** oder **Jugendlicher**), das Sie anpassen möchten, auf die Schaltfläche **Einstellungen**.
5. Aktivieren Sie im folgenden Fenster **Profil anpassen** auf der Registerkarte **Erweitert** das Kontrollkästchen **Heuristische Analyse verwenden** und stellen Sie darunter mit Hilfe des Schiebereglers die Genauigkeitsstufe der Analyse ein.

AKTION BEI EINEM ZUGRIFFSVERSUCH AUF VERBOTENE WEBADRESSEN AUSWÄHLEN

Wenn ein Benutzer versucht, Zugriff auf eine verbotene Internetressource zu erhalten, führt die Kindersicherung die vorgegebene Aktion aus.

Gehen Sie folgendermaßen vor, um die Aktion auszuwählen, die von der Komponente bei einem Zugriffsversuch auf eine verbotene Webressource ausgeführt werden soll:

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Kindersicherung** aus.
3. Klicken Sie für die ausgewählte Komponente auf die Schaltfläche **Einstellungen**.
4. Wählen Sie im folgenden Fenster auf der Registerkarte des erforderlichen Profils (**Kind** oder **Jugendlicher**) im entsprechenden Block eine Aktion aus.

ZEITBESCHRÄNKUNG FÜR DEN ZUGRIFF

Sie können die Zeit, die ein Benutzer im Internet verbringen darf, beschränken. Dabei sind drei Arten der Beschränkung möglich. In der Grundeinstellung sind die Beschränkungsbedingungen durch die Parameter für Anzeige festgelegt. Die Parameter für die Zeitbeschränkung lassen sich in 30 Minuten Schritten anpassen. Neben einem Zeitplan kann auch die Gesamtdauer beschränkt werden, während der der Internetzugriff erlaubt sein soll.

Beispiel:

Sie haben für das Profil **Kind** die tägliche Arbeitszeit im Internet auf drei Stunden beschränkt, den Internetzugriff aber zusätzlich nur von 14:00 bis 15:00 Uhr erlaubt. In diesem Fall wird der Zugriff auf Webseiten nur während des festgelegten Zeitraums erlaubt und die Anzahl der erlaubten Stunden wird ignoriert.

Gehen Sie folgendermaßen vor, um die Dauer für den Internetzugriff zu beschränken:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.

2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Kindersicherung** aus.

3. Klicken Sie für die ausgewählte Komponente auf die Schaltfläche **Einstellungen**.

4. Klicken Sie auf der Registerkarte des Profils (**Kind** oder **Jugendlicher**), das Sie anpassen möchten, auf die Schaltfläche **Einstellungen**.

5. Legen Sie im folgenden Fenster **Profil anpassen** auf der Registerkarte **Zeitplan** die entsprechenden Parameter fest.

   Um die tägliche Gesamtdauer für die Arbeit im Internet zu beschränken, aktivieren Sie das Kontrollkästchen **Tägliche Arbeitszeit im Internet beschränken** und geben Sie die Beschränkungsbedingungen an.

   Der Zeitplan für den Internetzugriff wird durch farbliche Hervorhebung der entsprechenden Zeiträume in der Tabelle festgelegt. Die Tabellenzeilen entsprechen den Wochentagen, die Spalten jeweils einem Zeitraum von 30 Minuten auf einer Zeitskala. Abhängig von den regionalen Zeitparametern, die ihn Ihrem Betriebssystem eingestellt sind, kann die Zeitskala das 12- oder 24-Stundenformat besitzen. Die Farben der Tabellenzellen symbolisieren die festgelegten Beschränkungen: Rot bedeutet, der Zugriff auf Internetressourcen ist verboten, Grün – der Zugriff ist erlaubt, und Gelb – der Zugriff ist nach den geltenden Restriktionen (s. S. 130) beschränkt.

   Wenn Sie beide Methoden zur Zeitbeschränkung festgelegt haben und ein zeitlicher Wert den anderen überschreitet, wird der kleinere Wert verwendet.

UNTERSUCHUNG DES COMPUTERS

Die Untersuchung des Computers auf Viren und Schwachstellen ist eine der wichtigsten Funktionen für die Sicherheit des Rechners. Durch die Virensuche lässt sich die Ausbreitung von schädlichem Code erkennen, der aus bestimmten Gründen nicht vom Malware-Schutz erkannt wurde. Durch die Schwachstellen-Suche wird in Programmen das Vorhandensein von Sicherheitslücken erkannt, die Angreifern zur Verbreitung schädlicher Objekte und zum Zugriff auf persönliche Daten dienen können.

Die Fachleute von Kaspersky Lab haben die Aufgaben Virenuntersuchung (s. S. 136) entwickelt, darunter die Untersuchung von Wechseldatenträgern (s. S. 142) sowie die Aufgabe Suche nach Schwachstellen im System und in Programmen (s. S. 147).

Gehen Sie folgendermaßen vor, um die Parameter einer bestimmten Untersuchungsaufgabe zu ändern:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.

2. Wählen Sie auf der linken Seite des Fensters im Abschnitt **Untersuchung** die erforderliche Aufgabe aus (**Vollständige Untersuchung**, **Schnelle Untersuchung**, **Untersuchung von Objekten**, **Suche nach Schwachstellen**).

3. Nehmen Sie für die ausgewählte Aufgabe die erforderlichen Änderungen vor.

IN DIESEM ABSCHNITT

Virensuche 136

Suche nach Schwachstellen..... 147

VIRENSUCHE

Die Spezialisten von Kaspersky Lab haben folgende Aufgaben für die Virenuntersuchung Ihres Computers vordefiniert.

- **Objekte untersuchen**. Es werden die vom Benutzer festlegten Objekte untersucht. Es kann ein beliebiges Objekt des Dateisystems auf dem Computer untersucht werden. Im Rahmen dieser Aufgabe können Sie die Parameter anpassen, die für die Untersuchung von Wechseldatenträgern gelten.

- **Vollständige Untersuchung**. Ausführliche Untersuchung des Systems. Standardmäßig werden folgende Objekte untersucht: Systemspeicher, Objekte, die beim Systemstart gestartet werden, Systemwiederherstellung, Mail-Datenbanken, Festplatten, Wechseldatenträger und Netzlaufwerke.

- **Schnelle Untersuchung**. Es werden die Objekte untersucht, die beim Hochfahren des Betriebssystems gestartet werden.

Die Aufgaben zur vollständigen und schnellen Untersuchung sind spezifische Aufgaben. Es wird davor gewarnt, die Liste der Untersuchungsobjekte für diese Aufgaben zu ändern.

Jeder Untersuchungsaufgabe wird in einem bestimmten Bereich ausgeführt und kann nach einem festgelegten Zeitplan gestartet werden. Die Parameter von Aufgaben zur Virensuche sind von der Sicherheitsstufe abhängig. Es sind drei vordefinierte Stufen vorgesehen.

Nach dem Start einer Aufgabe zur Virensuche wird im Hauptfenster von Kaspersky Internet Security ihr Status im Abschnitt **Untersuchung** im Feld **Letzter Start** unter dem Namen der gestarteten Aufgabe angezeigt. Beim Fund einer Bedrohung führt die Anwendung eine festgelegte Aktion aus.

Während die Virensuche ausgeführt wird, werden Informationen über ihre Ergebnisse im Bericht von Kaspersky Internet Security aufgezeichnet.

Außerdem können Sie ein Untersuchungsobjekt mit den Standardmitteln des Betriebssystems Microsoft Windows (beispielsweise im Fenster des Programms **Explorer** oder auf dem **Arbeitsplatz** usw.) auswählen. Führen Sie dazu den Mauszeiger auf den Namen des gewünschten Objekts, öffnen Sie mit der rechten Maustaste das Microsoft Windows-Kontextmenü und wählen Sie den Punkt **Auf Viren untersuchen** aus.

Abbildung 9: Kontextmenü von Microsoft Windows

Außerdem können Sie zum Bericht über die Untersuchung wechseln, der vollständige Informationen über die Ereignisse, die bei der Ausführung von Aufgaben eingetreten sind, bietet.

SIEHE AUCH

Start der Untersuchungsaufgabe 138

Verknüpfung für den Aufgabenstart erstellen 139

Liste der Untersuchungsobjekte erstellen 139

Sicherheitsstufe ändern 140

Aktion beim Fund einer Bedrohung ändern 140

Typ der zu untersuchenden Objekte ändern 141

Untersuchung optimieren 142

Wechseldatenträger untersuchen 142

Untersuchung von zusammengesetzten Dateien 143

Untersuchungstechnologie 144

Untersuchungsmethode ändern 144

Startmodus: Zeitplan erstellen 145

Startmodus: Benutzerkonto festlegen 145

Besonderheiten beim Start von geplanten Untersuchungsaufgaben 146

Standardmäßige Untersuchungseinstellungen wiederherstellen 146

START DER UNTERSUCHUNGSAUFGABE

Für den Start einer Untersuchungsaufgabe stehen folgende Möglichkeiten zur Verfügung:

- aus dem Kontextmenü (s. Abschnitt "Kontextmenü " auf S. 42) von Kaspersky Internet Security.
- aus dem Hauptfenster (s. Abschnitt "Hauptfenster von Kaspersky Internet Security" auf S. 43) von Kaspersky Internet Security.
- mit einer zuvor hergestellten Verknüpfung (s. S. 139).

Informationen über den Verlauf der Aufgabenausführung werden im Hauptfenster von Kaspersky Internet Security angezeigt.

Außerdem können Sie ein Untersuchungsobjekt mit den Standardmitteln des Betriebssystems Microsoft Windows (beispielsweise im Fenster des Programms **Explorer** oder auf dem **Arbeitsplatz** usw.) auswählen.

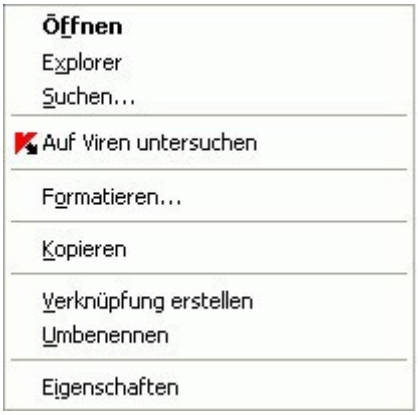

Abbildung 10: Kontextmenü von Microsoft Windows

Gehen Sie folgendermaßen vor, um eine Aufgabe mit Hilfe einer Verknüpfung zu starten:

1. Öffnen Sie den Ordner, in dem Sie die Verknüpfung erstellt haben.
2. Starten Sie die Aufgabe durch Doppelklick auf die Verknüpfung. Informationen über die Aufgabenausführung werden im Hauptfenster von Kaspersky Internet Security im Abschnitt **Untersuchung** angezeigt.

Gehen Sie folgendermaßen vor, um eine Aufgabe zur Virensuche aus dem Kontextmenü des Programms zu starten:

1. Klicken Sie im Infobereich der Taskleiste mit der rechten Maustaste auf das Programmsymbol.
2. Wählen Sie im Kontextmenü den Punkt **Auf Viren untersuchen**.
3. Klicken Sie im folgenden Fenster von Kaspersky Internet Security im Abschnitt **Untersuchung** auf die Schaltfläche mit dem Namen der entsprechenden Aufgabe.

Um die vollständige Untersuchung des Computers zu starten, wählen Sie im Kontextmenü den Punkt **Computer vollständig untersuchen** aus. Die vollständige Untersuchung des Computers wird gestartet. Informationen über die Aufgabenausführung werden im Hauptfenster von Kaspersky Internet Security im Abschnitt **Untersuchung** angezeigt.

Gehen Sie folgendermaßen vor, um eine Aufgabe zur Virensuche aus dem Programmhauptfenster zu starten:

1. Öffnen Sie das Programmhauptfenster.
2. Wählen Sie auf der linken Fensterseite den Abschnitt **Untersuchung**.
3. Klicken Sie auf die Schaltfläche mit dem Namen der entsprechenden Aufgabe.

Gehen Sie folgendermaßen vor, um eine Aufgabe zur Virensuche für eine ausgewähltes Objekt aus dem Kontextmenü von Microsoft Windows zu starten:

1. Klicken Sie mit der rechten Maustaste auf den Namen des gewählten Objekts.

2. Wählen Sie im Kontextmenü den Punkt **Auf Viren untersuchen**. Der Fortschritt und das Ergebnis der Aufgabenausführung werden im folgenden Fenster dargestellt.

VERKNÜPFUNG FÜR DEN AUFGABENSTART ERSTELLEN

Zum schnellen Start der Aufgaben zur vollständigen und schnellen Untersuchung ist im Programm die Möglichkeit vorgesehen, eine Verknüpfung anzulegen. So kann die erforderliche Untersuchungsaufgabe gestartet werden, ohne das Programmhauptfenster oder das Kontextmenü zu öffnen.

Gehen Sie folgendermaßen vor, um eine Verknüpfung für den Start einer Untersuchungsaufgabe zu erstellen:

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.

2. Wählen Sie auf der linken Fensterseite den Abschnitt **Untersuchung**.

3. Klicken Sie auf der rechten Seite des Fensters im Block **Schneller Aufgabenstart** neben dem entsprechenden Aufgabennamen **(Schnelle Untersuchung** oder **Vollständige Untersuchung**) auf die Schaltfläche **Verknüpfung erstellen**.

4. Geben Sie im folgenden Fenster an, wo und unter welchem Namen die Verknüpfung gespeichert werden soll. Standardmäßig wird die Verknüpfung unter dem Aufgabennamen im Ordner *Arbeitsplatz* des aktiven Computerbenutzers erstellt.

LISTE DER UNTERSUCHUNGSOBJEKTE ERSTELLEN

Standardmäßig entspricht jeder Aufgabe zur Virensuche eine eigene Liste von Objekten. Zu diesen Objekten können sowohl Objekte des Computerdateisystems (z.B. logische Laufwerke, **Mail-Datenbanken**), als auch Objekte anderer Typen (z.B. Netzlaufwerke) gehören. Diese Liste kann geändert werden.

Das hinzugefügte Objekt erscheint sofort in der Liste. Wenn beim Hinzufügen eines Objekts das Kontrollkästchen **Unterordner einschließen** aktiviert wurde, wird die Untersuchung rekursiv ausgeführt.

Um ein Objekt aus der Liste zu entfernen, verwenden Sie den Link **Löschen**.

Objekte, die sich standardmäßig in der Liste befinden, können nicht geändert oder gelöscht werden.

Objekte können vorübergehend von der Untersuchung ausgeschlossen werden, ohne aus der Liste gelöscht zu werden. Markieren Sie dazu das Objekt in der Liste und deaktivieren Sie das Kontrollkästchen links vom Namen des Objekts.

Wenn der Untersuchungsbereich leer ist oder kein Objekt des Untersuchungsbereichs angekreuzt wurde, kann die Untersuchungsaufgabe nicht gestartet werden!

Gehen Sie folgendermaßen vor, um für eine Untersuchungsaufgabe eine Liste der Untersuchungsobjekte zu erstellen:

1. Öffnen Sie das Programmhauptfenster.

2. Wählen Sie auf der linken Fensterseite den Abschnitt **Untersuchung**.

3. Klicken Sie auf den Link **Hinzufügen**.

4. Wählen Sie im folgenden Fenster **Untersuchungsobjekt auswählen** ein Objekt aus und klicken sie auf die Schaltfläche **Hinzufügen**. Nachdem alle erforderlichen Objekte hinzugefügt wurden, klicken Sie auf **OK**. Um bestimmte Objekte aus der Untersuchungsliste auszuschließen, deaktivieren Sie das entsprechende Kontrollkästchen.

Gehen Sie folgendermaßen vor, um für eine Aufgabe zur schnellen oder vollständigen Untersuchung eine Liste mit Untersuchungsobjekten zu erstellen:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.

2. Wählen Sie auf der linken Fensterseite die Aufgabe **Vollständige Untersuchung** (**Schnelle Untersuchung**) aus.

3. Klicken Sie für die ausgewählte Aufgabe im Block **Untersuchungsobjekte** auf die Schaltfläche **Einstellungen**.

4. Erstellen Sie im folgenden Fenster **<Name der Untersuchungsaufgabe>: Liste der Objekte** mit Hilfe der Links **Hinzufügen**, **Ändern** und **Löschen** eine Liste. Um bestimmte Objekte aus der Untersuchungsliste auszuschließen, deaktivieren Sie das entsprechende Kontrollkästchen.

SICHERHEITSSTUFE ÄNDERN

Unter Sicherheitsstufe wird eine vordefinierte Auswahl von Untersuchungsparametern verstanden. Die Spezialisten von Kaspersky Lab haben drei Sicherheitsstufen vordefiniert. Bei der Auswahl der Sicherheitsstufe sollten Sie die aktuelle Situation berücksichtigen. Folgende Sicherheitsstufen stehen zur Auswahl:

- **Hoch**. Sie sollte verwendet werden, wenn Sie das Infektionsrisiko für Ihren Computer sehr hoch einschätzen.

- **Empfohlen**. Diese Stufe ist in den meisten Fällen geeignet und wird von den Kaspersky-Lab-Spezialisten empfohlen.

- **Niedrig**. Wenn Sie mit Programmen arbeiten, die den Arbeitsspeicher stark beanspruchen, wählen Sie die niedrige Sicherheitsstufe aus, da die Auswahl der untersuchten Dateien auf dieser Stufe eingeschränkt wird.

Wenn keine der vordefinierten Stufen Ihren Anforderungen entspricht, können Sie die Untersuchungsparameter anpassen. Dadurch ändert sich der Name der Sicherheitsstufe in **Benutzerdefiniert**. Um die standardmäßigen Einstellungen der Komponente wiederherzustellen, wählen Sie eine der vordefinierten Stufen aus.

Gehen Sie folgendermaßen vor, um die festgelegte Sicherheitsstufe zu ändern:

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.

2. Wählen Sie auf der linken Seite des Fensters im Abschnitt **Untersuchung** die erforderliche Aufgabe aus (**Vollständige Untersuchung**, **Schnelle Untersuchung**, **Untersuchung von Objekten**).

3. Stellen Sie für die ausgewählte Aufgabe im Block **Sicherheitsstufe** die erforderliche Sicherheitsstufe ein.

AKTION BEIM FUND EINER BEDROHUNG ÄNDERN

Beim Fund einer Bedrohung weist Kaspersky Internet Security dieser einen der folgenden Statusvarianten zu:

- Status eines der schädlichen Programme (beispielsweise *Virus*, *trojanisches Programm*).

- Status *möglicherweise infiziert*, wenn sich aufgrund der Untersuchung nicht eindeutig feststellen lässt, ob das Objekt infiziert ist oder nicht. Möglicherweise wurde in der Datei der Code eines unbekannten Virus oder der modifizierte Code eines bekannten Virus gefunden.

Wenn Kaspersky Internet Security bei einer Untersuchung infizierte oder möglicherweise infizierte Objekte findet, werden Sie darüber informiert. Auf dem Fund einer Bedrohung muss reagiert werden, indem eine Aktion für das Objekt

ausgewählt wird. Standardmäßig ist in Kaspersky Internet Security als Aktion für ein gefundenes Objekt die Variante **Aktion erfragen** festgelegt. Sie können die Aktion ändern. Wenn Sie beispielsweise sicher sind, dass versucht werden soll, alle gefundenen Objekte zu desinfizieren, und bei einer Meldung über den Fund eines infizierten oder verdächtigen Objekts nicht jedes Mal die Aktion **Desinfizieren** auswählen möchten, dann legen Sie folgende Aktion fest: **Aktion ausführen. Desinfizieren**.

Bevor ein infiziertes Objekt desinfiziert oder gelöscht wird, legt Kaspersky Internet Security eine Sicherungskopie des Objekts an. Dadurch wird erlaubt, das Objekt bei Bedarf wiederherzustellen oder später zu desinfizieren.

Wenn Sie im automatischen Modus (s. Abschnitt "Schritt 2. Schutzmodus auswählen" auf S. 32) arbeiten, wendet Kaspersky Internet Security automatisch die von den Kaspersky-Lab-Fachleuten empfohlene Aktion an, wenn gefährliche Objekte erkannt werden. Für schädliche Objekte ist dies die Aktion **Desinfizieren. Löschen, wenn Desinfektion nicht möglich**, für verdächtige Objekte ist es **Überspringen**.

Gehen Sie folgendermaßen vor, um die festgelegte Aktion für gefundene Objekte zu ändern:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie auf der linken Seite des Fensters im Abschnitt **Untersuchung** die erforderliche Aufgabe aus (**Vollständige Untersuchung**, **Schnelle Untersuchung**, **Untersuchung von Objekten**).
3. Geben Sie für die ausgewählte Aufgabe im Block **Aktion** die erforderliche Aktion an.

TYP DER ZU UNTERSUCHENDEN OBJEKTE ÄNDERN

Durch die Angabe des Typs der zu untersuchenden Objekte bestimmen Sie das Format und die Größe der Dateien, die beim Ausführen der gewählten Aufgabe untersucht werden sollen.

Bei der Auswahl des Dateityps sollten folgende Besonderheiten beachtet werden:

- Es gibt eine Reihe von Dateiformaten (z.B. *txt*), für die das Risiko des Eindringens von schädlichem Code und dessen späterer Aktivierung relativ gering ist. Gleichzeitig gibt es Formate, die ausführbaren Code enthalten oder enthalten können (*exe*, *dll*, *doc*). Das Risiko des Eindringens und der Aktivierung von schädlichem Code ist für solche Dateien relativ hoch.
- Es sollte beachtet werden, dass ein Angreifer einen Virus in einer Datei mit der Erweiterung *txt* an Ihren Computer senden kann, obwohl es sich in Wirklichkeit um eine ausführbare Datei handelt, die in eine *txt*-Datei umbenannt wurde. Wenn die Variante **Dateien nach Erweiterung untersuchen** gewählt wurde, wird eine solche Datei bei der Untersuchung übersprungen. Wenn die Variante **Dateien nach Format untersuchen** gewählt wurde, ignoriert der Dateischutz die Erweiterung und analysiert die Kopfzeile der Datei, wodurch sich herausstellen kann, dass die Datei das Format exe besitzt. Eine solche Datei wird der sorgfältigen Virusuntersuchung unterzogen.

Gehen Sie folgendermaßen vor, um den Typ der zu untersuchenden Dateien zu ändern:

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
2. Wählen Sie auf der linken Seite des Fensters im Abschnitt **Untersuchung** die erforderliche Aufgabe aus (**Vollständige Untersuchung**, **Schnelle Untersuchung**, **Untersuchung von Objekten**).
3. Klicken Sie für die ausgewählte Aufgabe im Block **Sicherheitsstufe** auf die Schaltfläche **Einstellungen**.
4. Wählen Sie im folgenden Fenster auf der Registerkarte **Gültigkeitsbereich** im Block **Dateitypen** den gewünschten Parameter.

UNTERSUCHUNG OPTIMIEREN

Sie können die Untersuchungszeit verkürzen und die Arbeitsgeschwindigkeit von Kaspersky Internet Security erhöhen. Damit nur neue Dateien und Dateien, die seit der letzten Analyse verändert wurden, untersucht werden: Dieser Untersuchungsmodus erstreckt sich auf gewöhnliche und zusammengesetzte Dateien.

Außerdem kann die Untersuchungsdauer beschränkt werden. Nach Ablauf der festgelegten Zeit, wird die Dateiuntersuchung abgebrochen.

Gehen Sie folgendermaßen vor, damit nur neue und veränderte Dateien untersucht werden:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie auf der linken Seite des Fensters im Abschnitt **Untersuchung** die erforderliche Aufgabe aus (**Vollständige Untersuchung**, **Schnelle Untersuchung**, **Untersuchung von Objekten**).
3. Klicken Sie für die ausgewählte Aufgabe im Block **Sicherheitsstufe** auf die Schaltfläche **Einstellungen**.
4. Aktivieren Sie im folgenden Fenster auf der Registerkarte **Gültigkeitsbereich** im Block **Untersuchung optimieren** das Kontrollkästchen **Nur neue und veränderte Dateien untersuchen**.

Gehen Sie folgendermaßen vor, um eine zeitliche Begrenzung für die Untersuchung festzulegen:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie auf der linken Seite des Fensters im Abschnitt **Untersuchung** die erforderliche Aufgabe aus (**Vollständige Untersuchung**, **Schnelle Untersuchung**, **Untersuchung von Objekten**).
3. Klicken Sie für die ausgewählte Aufgabe im Block **Sicherheitsstufe** auf die Schaltfläche **Einstellungen**.
4. Aktivieren Sie im folgenden Fenster auf der Registerkarte **Gültigkeitsbereich** im Block **Untersuchung optimieren** das Kontrollkästchen **Untersuchung beenden, wenn länger als** und geben Sie im Feld daneben die Untersuchungsdauer an.

WECHSELDATENTRÄGER UNTERSUCHEN

In letzter Zeit treten vermehrt schädliche Objekte auf, die Schwachstellen des Betriebssystems ausnutzen, um sich über lokale Netzwerke und Wechseldatenträger auszubreiten.

Verwenden Sie eine Funktion, mit der Wechseldatenträger untersucht werden, wenn sie an den Computer angeschlossen werden. Wählen Sie dazu eine Aktion aus, die Kaspersky Internet Security ausführen soll:

- **Nicht untersuchen**. Wenn Wechseldatenträger an den Computer angeschlossen werden, erfolgt keine Untersuchung.
- **Benutzer fragen**. In der Grundeinstellung werden Sie von Kaspersky Internet Security nach dem weiteren Vorgehen gefragt, wenn ein Wechseldatenträger angeschlossen wird.
- **Vollständige Untersuchung**. Wenn Wechseldatenträger angeschlossen werden, erfolgt eine vollständige Untersuchung der darauf gespeicherten Dateien. Dabei werden die Parameter der Aufgabe Vollständige Untersuchung verwendet.
- **Schnelle Untersuchung**. Wenn Wechseldatenträger angeschlossen werden, erfolgt nur eine Untersuchung der Autostart-Objekte. Dabei werden die Parameter der Aufgabe Schnelle Untersuchung verwendet.

Gehen Sie folgendermaßen vor, um die Option zur Untersuchung von Wechseldatenträgern zu verwenden, wenn diese an den Computer angeschlossen werden:

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.

2. Wählen Sie auf der linken Fensterseite den Abschnitt **Untersuchung**.

3. Wählen Sie im Block **Wechseldatenträger beim Anschließen untersuchen** eine Aktion aus und begrenzen Sie bei Bedarf im Feld unten die Größe der zu untersuchenden Laufwerke.

UNTERSUCHUNG VON ZUSAMMENGESETZTEN DATEIEN

Eine häufige Methode zum Verstecken von Viren ist das Eindringen von Schädlingen in zusammengesetzte Dateien wie Archive, Datenbanken usw. Um Viren zu erkennen, die auf diese Weise versteckt wurden, muss eine zusammengesetzte Datei entpackt werden. Dadurch kann das Untersuchungstempo wesentlich sinken.

Für jeden Typ einer zusammengesetzten Datei können Sie auswählen, ob alle oder nur neue Dateien untersucht werden sollen. Verwenden Sie dazu den Link neben dem Namen des Objekts. Der Link verändert seinen Wert, wenn mit der linken Maustaste darauf geklickt wird. Wenn festgelegt wurde, dass nur neue und veränderte Dateien untersucht werden sollen (s. S. 142), steht die Auswahl des Typs der zusammengesetzten Dateien nicht zur Verfügung.

Außerdem können Sie festlegen, bis zu welcher maximalen Größe eine zusammengesetzte Datei untersucht werden soll. Zusammengesetzte Dateien, die die festgelegte Größe überschreiten, werden nicht untersucht.

Beim Extrahieren aus Archiven werden Dateien auch dann untersucht, wenn das Kontrollkästchen ☑ **Große zusammengesetzte Dateien nicht entpacken** aktiviert ist.

Gehen Sie folgendermaßen vor, um Liste der zu untersuchenden zusammengesetzten Dateien zu ändern:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.

2. Wählen Sie auf der linken Seite des Fensters im Abschnitt **Untersuchung** die erforderliche Aufgabe aus (**Vollständige Untersuchung**, **Schnelle Untersuchung**, **Untersuchung von Objekten**).

3. Klicken Sie für die ausgewählte Aufgabe im Block **Sicherheitsstufe** auf die Schaltfläche **Einstellungen**.

4. Wählen Sie im folgenden Fenster auf der Registerkarte **Gültigkeitsbereich** im Block **Untersuchung von zusammengesetzten Dateien** den erforderlichen Typ für die zu untersuchenden zusammengesetzten Dateien.

Gehen Sie folgendermaßen vor, um eine maximale Größe für zusammengesetzte Dateien festzulegen, die untersucht werden sollen:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.

2. Wählen Sie auf der linken Seite des Fensters im Abschnitt **Untersuchung** die erforderliche Aufgabe aus (**Vollständige Untersuchung**, **Schnelle Untersuchung**, **Untersuchung von Objekten**).

3. Klicken Sie für die ausgewählte Aufgabe im Block **Sicherheitsstufe** auf die Schaltfläche **Einstellungen**.

4. Klicken Sie im folgenden Fenster auf der Registerkarte **Gültigkeitsbereich** im Block **Untersuchung von zusammengesetzten Dateien** auf die Schaltfläche **Erweitert**.

5. Aktivieren Sie im folgenden Fenster **Zusammengesetzte Dateien** das Kontrollkästchen ☑ **Große zusammengesetzte Dateien nicht entpacken** und legen Sie darunter im Feld die maximale Größe für zu untersuchende Dateien fest.

UNTERSUCHUNGSTECHNOLOGIE

Zusätzlich können Sie eine Technologie auswählen, die bei der Untersuchung verwendet werden soll: Folgende Technologien stehen zur Auswahl:

- **iChecker**. Eine Technologie, die eine Steigerung der Untersuchungsgeschwindigkeit erlaubt, indem bestimmte Objekte ausgeschlossen werden. Das Ausschließen eines Objekts von der Untersuchung erfolgt nach einem speziellen Algorithmus, der das Erscheinungsdatum der Programm-Datenbanken, das Datum der letzten Untersuchung des Objekts und die Änderung von Untersuchungsparametern berücksichtigt.

  Eine Archivdatei wurde beispielsweise von Kaspersky Internet Security untersucht und ihr wurde der Status *virenfrei* zugewiesen. Dann wird das Archiv von der folgenden Untersuchung ausgeschlossen, wenn es nicht verändert wurde und die Untersuchungsparameter gleich geblieben sind. Wenn seit der letzten Untersuchung die Zusammensetzung des Archivs durch Hinzufügen eines neuen Objekts verändert wurde, die Untersuchungsparameter geändert oder die Programm-Datenbanken aktualisiert wurden, wird das Archiv erneut untersucht.

  Die Technologie iChecker besitzt folgende Einschränkungen: Sie funktioniert nicht mit umfangreichen Dateien und kann nur auf Objekte angewandt werden, deren Struktur dem Programm bekannt ist (z.B. die Dateiformate exe, dll, lnk, ttf, inf, sys, com, chm, zip, rar).

- **iSwift**. Diese Technologie stellt eine Weiterentwicklung der iChecker-Technologie für Computer mit NTFS-Dateisystem dar. Die Technologie iSwift besitzt folgende Einschränkungen: Sie ist an einen konkreten Ort der Datei im Dateisystem gebunden und kann nur auf Objekte angewandt werden, die sich in einem NTFS-Dateisystem befinden.

➡ *Gehen Sie folgendermaßen vor, um die Untersuchungstechnologie für Objekte zu ändern:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.

2. Wählen Sie auf der linken Seite des Fensters im Abschnitt **Untersuchung** die erforderliche Aufgabe aus (**Vollständige Untersuchung**, **Schnelle Untersuchung**, **Untersuchung von Objekten**).

3. Klicken Sie für die ausgewählte Aufgabe im Block **Sicherheitsstufe** auf die Schaltfläche **Einstellungen**.

4. Wählen Sie im folgenden Fenster auf der Registerkarte **Erweitert** im Block **Untersuchungstechnologien** den erforderlichen Parameterwert.

UNTERSUCHUNGSMETHODE ÄNDERN

Sie können die Untersuchungsparameter anpassen, die die Ausführlichkeit der Untersuchung beeinflussen. In der Grundeinstellung ist immer der Untersuchungsmodus mit Hilfe der Anti-Viren-Datenbanken des Programms aktiviert. Außerdem lassen sich verschiedene Verfahren und Technologien der Untersuchung (s. S. 144) aktivieren.

Der Suchmodus, in dem Kaspersky Internet Security ein gefundenes Objekt mit den Einträgen in den Datenbanken vergleicht, heißt *Signaturanalyse* und wird immer verwendet. Außerdem können Sie die *heuristische Analyse* verwenden. Diese Methode umfasst die Analyse der Aktivität, die ein Objekt im System zeigt. Wenn die erkannte Aktivität als typisch für schädliche Objekte gilt, lässt sich das Objekt mit hoher Wahrscheinlichkeit als schädlich oder verdächtig einstufen.

Zusätzlich kann die Genauigkeitsstufe der heuristischen Analyse ausgewählt werden: oberflächlich, mittel oder tief. Bewegen Sie dazu den Schieberegler auf die gewünschte Position.

Neben diesen Untersuchungsmethoden steht noch die Rootkit-Suche zur Verfügung. Ein Rootkit ist eine Kombination von Utilities, die schädliche Programme im Betriebssystem verstecken. Solche Tools dringen in das System ein. Sie tarnen ihre eigene Existenz und verstecken im System die Prozesse, Ordner oder Registrierungsschlüssel anderer Malware, die in der Konfiguration des Rootkits beschrieben ist. Wenn die Rootkit-Suche aktiviert ist, können Sie die Detailstufe für die Suche nach Rootkits auswählen. Aktivieren Sie dazu das Kontrollkästchen Erweiterte Analyse. In diesem Fall wird die ausführliche Suche nach solchen Programmen ausgeführt, wobei eine große Anzahl von Objekten unterschiedlicher Typen analysiert wird.

Gehen Sie folgendermaßen vor, um die erforderlichen Untersuchungsmethoden zu verwenden:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie auf der linken Seite des Fensters im Abschnitt **Untersuchung** die erforderliche Aufgabe aus (**Vollständige Untersuchung**, **Schnelle Untersuchung**, **Untersuchung von Objekten**).
3. Klicken Sie für die ausgewählte Aufgabe im Block **Startmodus** auf die Schaltfläche **Einstellungen**.
4. Wählen Sie im folgenden Fenster auf der Registerkarte **Erweitert** im Block **Untersuchungsmethoden** die gewünschten Parameterwerte.

STARTMODUS: ZEITPLAN ERSTELLEN

Es kann ein Zeitplan für den automatischen Start einer Untersuchungsaufgabe angelegt werden.

Die wichtigste Einstellung ist die Frequenz, mit der der Aufgabenstart erfolgen soll. Dazu ist es erforderlich, die Zeitplanparameter für die gewählte Variante anzugeben.

Wenn der Start aus irgendeinem Grund nicht möglich war (wenn beispielsweise der Computer im betreffenden Moment ausgeschaltet war), können Sie festlegen, dass der Start automatisch zum nächstmöglichen Zeitpunkt erfolgt.

Gehen Sie folgendermaßen vor, um den Startzeitplan einer Untersuchungsaufgabe anzupassen:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie auf der linken Seite des Fensters im Abschnitt **Untersuchung** die erforderliche Aufgabe aus (**Vollständige Untersuchung**, **Schnelle Untersuchung**, **Untersuchung von Objekten**).
3. Klicken Sie für die ausgewählte Aufgabe im Block **Startmodus** auf die Schaltfläche **Einstellungen**.
4. Wählen Sie im folgenden Fenster auf der Registerkarte **Startmodus** im Block **Zeitplan** die Variante **Manuell** aus, wenn Sie die Untersuchungsaufgabe zu einem geeigneten Zeitpunkt auf Befehl starten möchten. Damit die Aufgabe regelmäßig ausgeführt wird, wählen Sie die Variante **Zeitplan** aus und legen Sie einen Zeitplan für den Aufgabenstart fest.

Gehen Sie folgendermaßen vor, um den automatischen Start einer übersprungenen Aufgabe anzupassen:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie auf der linken Seite des Fensters im Abschnitt **Untersuchung** die erforderliche Aufgabe aus (**Vollständige Untersuchung**, **Schnelle Untersuchung**, **Untersuchung von Objekten**).
3. Klicken Sie für die ausgewählte Aufgabe im Block **Startmodus** auf die Schaltfläche **Einstellungen**.
4. Aktivieren Sie im folgenden Fenster auf der Registerkarte **Startmodus** im Block **Zeitplan** das Kontrollkästchen **Übersprungene Aufgabe starten**.

STARTMODUS: BENUTZERKONTO FESTLEGEN

Sie können das Benutzerkonto festlegen, mit dessen Rechten die Suche ausgeführt werden soll.

Gehen Sie folgendermaßen vor, um ein Benutzerkonto festzulegen:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.

2. Wählen Sie auf der linken Seite des Fensters im Abschnitt **Untersuchung** die erforderliche Aufgabe aus (**Vollständige Untersuchung**, **Schnelle Untersuchung**, **Untersuchung von Objekten**).

3. Klicken Sie für die ausgewählte Aufgabe im Block **Startmodus** auf die Schaltfläche **Einstellungen**.

4. Aktivieren Sie im folgenden Fenster auf der Registerkarte **Startmodus** im Block **Benutzer** das Kontrollkästchen **Aufgabe starten mit Rechten des Benutzers**. Geben Sie darunter in den Feldern den Benutzernamen und das Kennwort an.

BESONDERHEITEN BEIM START VON GEPLANTEN UNTERSUCHUNGSAUFGABEN

Alle Untersuchungsaufgaben können auf Befehl oder nach einem festgelegten Zeitplan gestartet werden.

Für Aufgaben, die nach einem festgelegten Zeitplan gestartet werden, können Sie eine zusätzliche Option verwenden: *Geplante Untersuchung anhalten, wenn Bildschirmschoner inaktiv oder Computer nicht blockiert ist*. Diese Option erlaubt es, den Start einer Aufgabe zurückzustellen, bis der Benutzer seine Arbeit auf dem Computer beendet hat. Dadurch wird verhindert, dass eine Untersuchungsaufgabe Computerressourcen verbraucht, während diese für andere Aufgaben benötigt werden.

- *Gehen Sie folgendermaßen vor, damit die Untersuchung erst gestartet wird, nachdem der Benutzer seine Arbeit beendet hat:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.

2. Wählen Sie auf der linken Seite des Fensters im Abschnitt **Untersuchung** die erforderliche Aufgabe aus (**Vollständige Untersuchung**, **Schnelle Untersuchung**, **Untersuchung von Objekten**).

3. Klicken Sie für die ausgewählte Aufgabe im Block **Startmodus** auf die Schaltfläche **Einstellungen**.

4. Aktivieren Sie im folgenden Fenster auf der Registerkarte **Startmodus** im Block **Startmodus** das Kontrollkästchen **Geplante Untersuchung anhalten, wenn Bildschirmschoner inaktiv oder Computer nicht blockiert ist**.

STANDARDMÄßIGE UNTERSUCHUNGSEINSTELLUNGEN WIEDERHERSTELLEN

Während der Konfiguration der Parameter für die Aufgabenausführung können Sie jederzeit zu den empfohlenen Einstellungen zurückkehren. Diese gelten als optimal, werden von den Kaspersky-Lab-Spezialisten empfohlen und sind in der Sicherheitsstufe **Empfohlen** zusammengefasst.

- *Gehen Sie folgendermaßen vor, um die standardmäßigen Untersuchungseinstellungen für Objekte wiederherzustellen,*

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.

2. Wählen Sie auf der linken Seite des Fensters im Abschnitt **Untersuchung** die erforderliche Aufgabe aus (**Vollständige Untersuchung**, **Schnelle Untersuchung**, **Untersuchung von Objekten**).

3. Klicken Sie für die ausgewählte Aufgabe im Block **Sicherheitsstufe** auf die Schaltfläche **Standard**.

SUCHE NACH SCHWACHSTELLEN

Die Aufgabe zur Schwachstellen-Suche umfasst eine Diagnose der Systemsicherheit und die Suche nach potentiellen Schwachstellen, die Angreifer gewöhnlich ausnutzen, um Schaden anzurichten.

Im Rahmen der Schwachstellen-Suche wird das System analysiert und es wird in den Einstellungen des Betriebssystems und des Browsers nach Anomalien und Beschädigungen gesucht. Die Sicherheitsdiagnose berücksichtigt unter anderem folgende Aspekte: Suche nach Rootkits (Programme zur heimlichen Kontrolle eines gehackten Systems), Suche nach Schwachstellen in Diensten und Parametern, Sammeln von Informationen über Prozesse, Treiber usw.

Die Systemdiagnose kann eine gewisse Zeit beanspruchen. Anschließend werden die gesammelten Informationen analysiert. Das Ziel der Analyse besteht darin, die gefundenen Sicherheitsprobleme hinsichtlich ihrer Gefährlichkeit für das System zu bewerten.

Alle Probleme, die bei der Systemanalyse gefunden wurden, werden im Hinblick auf die von ihnen für das System ausgehende Gefahr eingeteilt. Für jede Gruppe von Problemen schlagen die Kaspersky-Lab-Spezialisten eine Auswahl von Aktionen vor, mit denen die Schwachstellen und kritischen Punkte im System behoben werden können. Die Probleme und die entsprechenden Aktionen sind in drei Gruppen unterteilt:

- *Ausdrücklich empfohlene Aktionen* können Probleme beheben, die eine ernsthafte Sicherheitsbedrohung darstellen. Es wird empfohlen, alle Aktionen dieser Gruppe auszuführen.

- *Empfohlene Aktionen* dienen zum Beheben von Problemen, die ein potentielles Risiko darstellen können. Es wird empfohlen, auch alle Aktionen dieser Gruppe auszuführen.

- *Zusätzliche Aktionen* dienen dazu, momentan ungefährliche Probleme zu beheben, die die Computersicherheit in Zukunft bedrohen können.

Das Ergebnis der Suche nach potentiellen Schwachstellen im Betriebssystem und in den auf dem Computer installierten Anwendungen besteht in direkten Links zu kritischen Patches (Updates für Anwendungen).

Nach dem Start der Aufgabe Suche nach Schwachstellen (s. S. 147) wird der Fortschritt im Programmhauptfenster und im Fenster **Suche nach Schwachstellen** im Feld **Letzter Start** angezeigt. Die bei der Untersuchung im System und in Programmen gefundenen Schwachstellen werden im gleichen Fenster auf den Registerkarten **Systemschwachstellen** und **Programme mit Schwachstellen** angezeigt.

Während die Virensuche ausgeführt wird, werden Informationen über ihre Ergebnisse im Bericht von Kaspersky Internet Security aufgezeichnet.

Analog zu den Aufgaben zur Virensuche kann auch für die Schwachstellen-Suche im Abschnitt **Suche nach Schwachstellen** des Programmkonfigurationsfensters einen Startzeitplan (s. S. 149) erstellt und eine Liste der Untersuchungsobjekte (s. S. 148) angelegt werden. In der Grundeinstellung sind die auf dem Computer installierten Anwendungen als Untersuchungsobjekt ausgewählt.

SIEHE AUCH

Aufgabe zur Suche nach Schwachstellen starten 147

Verknüpfung für den Aufgabenstart erstellen 148

Liste der Untersuchungsobjekte erstellen 148

Startmodus: Zeitplan erstellen 149

Startmodus: Benutzerkonto festlegen 150

AUFGABE ZUR SUCHE NACH SCHWACHSTELLEN STARTEN

Für den Start der Aufgabe zur Schwachstellen-Suche stehen folgende Möglichkeiten zur Verfügung:

- aus dem Hauptfenster (s. Abschnitt "Hauptfenster von Kaspersky Internet Security" auf S. 43) von Kaspersky Internet Security.

- mit einer zuvor hergestellten Verknüpfung (s. S. 148).

Die Daten zur Aufgabenausführung werden im Hauptfenster von Kaspersky Internet Security und im Fenster **Suche nach Schwachstellen** angezeigt.

Gehen Sie folgendermaßen vor, um eine Aufgabe mit Hilfe einer Verknüpfung zu starten:

1. Öffnen Sie den Ordner, in dem Sie die Verknüpfung erstellt haben.

2. Starten Sie die Aufgabe durch Doppelklick auf die Verknüpfung. Der Ausführungsfortschritt der Aufgabe wird im Programmhauptfenster dargestellt.

Gehen Sie folgendermaßen vor, um die Aufgabe zur Schwachstellen-Suche aus dem Programmfenster zu starten:

1. Öffnen Sie das Programmhauptfenster.

2. Wählen Sie auf der linken Fensterseite den Abschnitt **Untersuchung**.

3. Klicken Sie auf die Schaltfläche **Fenster zur Suche nach Schwachstellen öffnen**.

4. Klicken Sie im folgenden Fenster auf die Schaltfläche **Suche nach Schwachstellen ausführen**. Informationen über die Aufgabenausführung werden im Feld **Ende** angezeigt. Um die Aufgabenausführung abzubrechen, klicken Sie erneut auf die Schaltfläche.

VERKNÜPFUNG FÜR DEN AUFGABENSTART ERSTELLEN

Zum schnellen Start einer Aufgabe zur Suche nach Schwachstellen ist im Programm die Möglichkeit vorgesehen, eine Verknüpfung zu erstellen. So kann eine Aufgabe gestartet werden, ohne das Programmhauptfenster zu öffnen.

Gehen Sie folgendermaßen vor, um eine Verknüpfung für den Start der Aufgabe zur Suche nach Schwachstellen zu erstellen:

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.

2. Wählen Sie auf der linken Fensterseite den Abschnitt **Untersuchung**.

3. Klicken Sie auf der rechten Seite des Fensters im Block **Schneller Aufgabenstart** neben dem Aufgabennamen (**Suche nach Schwachstellen**) auf die Schaltfläche **Verknüpfung erstellen**.

4. Geben Sie im folgenden Fenster an, wo und unter welchem Namen die Verknüpfung gespeichert werden soll. Standardmäßig wird die Verknüpfung unter dem Aufgabennamen im Ordner *Arbeitsplatz* des aktiven Computerbenutzers erstellt.

LISTE DER UNTERSUCHUNGSOBJEKTE ERSTELLEN

Standardmäßig verfügt die Aufgabe zur Schwachstellen-Suche über eine eigene Liste von Untersuchungsobjekten. Zu diesen Objekten gehören das Betriebssystem und die auf dem Computer installierten Programme. Es können auch zusätzliche Untersuchungsobjekte angegeben werden: sowohl Objekte des Computerdateisystems (z.B. logische Laufwerke, **Mail-Datenbanken**), als auch Objekte anderer Typen (z.B. Netzlaufwerke).

Das hinzugefügte Objekt erscheint sofort in der Liste. Wenn beim Hinzufügen eines Objekts das Kontrollkästchen ☑ **Unterordner einschließen** aktiviert wurde, wird die Untersuchung rekursiv ausgeführt. Objekte, die manuell hinzugefügt wurden, werden ebenfalls der Virusuntersuchung unterzogen.

Um ein Objekt aus der Liste zu entfernen, verwenden Sie den Link **Löschen**.

Objekte, die sich standardmäßig in der Liste befinden, können nicht geändert oder gelöscht werden.

Objekte können vorübergehend von der Untersuchung ausgeschlossen werden, ohne aus der Liste gelöscht zu werden. Markieren Sie dazu das Objekt in der Liste und deaktivieren Sie das Kontrollkästchen links vom Namen des Objekts.

Wenn der Untersuchungsbereich leer ist oder kein Objekt des Untersuchungsbereichs angekreuzt wurde, kann die Untersuchungsaufgabe nicht gestartet werden!

Gehen Sie folgendermaßen vor, um eine Liste der Objekte für die Aufgabe zur Schwachstellen-Suche zu erstellen:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie auf der linken Seite des Fensters im Abschnitt **Untersuchung** die Aufgabe **Suche nach Schwachstellen** aus.
3. Klicken Sie für die ausgewählte Aufgabe im Block **Untersuchungsobjekte** auf die Schaltfläche **Einstellungen**.
4. Erstellen Sie im folgenden Fenster **Suche nach Schwachstellen: Liste der Objekte** mit Hilfe der Links **Hinzufügen**, **Ändern** und **Löschen** eine Liste. Um bestimmte Objekte aus der Untersuchungsliste auszuschließen, deaktivieren Sie das entsprechende Kontrollkästchen.

STARTMODUS: ZEITPLAN ERSTELLEN

Für die Aufgabe zur Schwachstellen-Suche kann ein Zeitplan für den automatischen Aufgabenstart erstellt werden.

Die wichtigste Einstellung ist die Frequenz, mit der die Aufgabe ausgeführt werden soll.

Wenn der Start aus irgendeinem Grund nicht möglich war (wenn beispielsweise der Computer im betreffenden Moment ausgeschaltet war), können Sie festlegen, dass der Start automatisch zum nächstmöglichen Zeitpunkt erfolgt.

Gehen Sie folgendermaßen vor, um den Startzeitplan einer Untersuchungsaufgabe anzupassen:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie auf der linken Seite des Fensters im Abschnitt **Untersuchung** die Aufgabe **Suche nach Schwachstellen** aus.
3. Klicken Sie für die ausgewählte Aufgabe im Block **Startmodus** auf die Schaltfläche **Einstellungen**.
4. Wählen Sie im folgenden Fenster auf der Registerkarte **Startmodus** im Block **Zeitplan** die Variante **Manuell** aus, wenn Sie die Untersuchungsaufgabe zu einem geeigneten Zeitpunkt auf Befehl starten möchten. Damit die Aufgabe regelmäßig ausgeführt wird, wählen Sie die Variante **Zeitplan** aus und legen Sie einen Zeitplan für den Aufgabenstart fest.

Gehen Sie folgendermaßen vor, um den automatischen Start einer übersprungenen Aufgabe anzupassen:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie auf der linken Seite des Fensters im Abschnitt **Untersuchung** die Aufgabe **Suche nach Schwachstellen** aus.
3. Klicken Sie für die ausgewählte Aufgabe im Block **Startmodus** auf die Schaltfläche **Einstellungen**.
4. Aktivieren Sie im folgenden Fenster auf der Registerkarte **Startmodus** im Block **Zeitplan** das Kontrollkästchen ☑ **Übersprungene Aufgabe starten**.

STARTMODUS: BENUTZERKONTO FESTLEGEN

Sie können das Benutzerkonto festlegen, mit dessen Rechten die Suche nach Schwachstellen ausgeführt werden soll.

Gehen Sie folgendermaßen vor, um ein Benutzerkonto festzulegen:

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.

2. Wählen Sie auf der linken Seite des Fensters im Abschnitt **Untersuchung** die Aufgabe **Suche nach Schwachstellen** aus.

3. Klicken Sie für die ausgewählte Aufgabe im Block **Startmodus** auf die Schaltfläche **Einstellungen**.

4. Aktivieren Sie im folgenden Fenster auf der Registerkarte **Startmodus** im Block **Benutzer** das Kontrollkästchen **Aufgabe starten mit Rechten des Benutzers**. Geben Sie darunter in den Feldern den Benutzernamen und das Kennwort an.

UPDATE

Eine Voraussetzung für die Sicherheit Ihres Computers besteht darin, den Schutz auf dem neusten Stand zu halten. Jeden Tag tauchen neue Viren, trojanische und andere schädliche Programme auf. Deshalb ist es sehr wichtig sicherzustellen, dass Ihre Informationen zuverlässig geschützt werden. Informationen über Bedrohungssignaturen und entsprechende Neutralisierungsmethoden sind in den Datenbanken von Kaspersky Internet Security enthalten. Deshalb stellt die regelmäßige Aktualisierung der Datenbanken einen sehr wichtigen Sicherheitsfaktor dar.

Die Aktualisierung des Programms umfasst den Download und die Installation folgender Elemente auf Ihren Computer:

- Datenbanken für Kaspersky Internet Security.

  Der Schutz der Informationen auf ihrem Computer basiert auf Datenbanken, die Beschreibungen von Bedrohungssignaturen und Netzwerkangriffen, sowie entsprechende Desinfektionsmethoden enthalten. Die Schutzkomponenten verwenden diese bei der Suche und Desinfektion gefährlicher Objekte auf Ihrem Computer. Die Datenbanken werden regelmäßig durch Einträge über neue Bedrohungen und entsprechende Desinfektionsmethoden ergänzt. Deshalb wird ausdrücklich empfohlen, die Datenbanken regelmäßig zu aktualisieren.

  Gemeinsam mit den Datenbanken von Kaspersky Internet Security werden auch die Netzwerktreiber aktualisiert, die die Funktionalität für das Abfangen des Netzwerkverkehrs durch die Schutzkomponenten gewährleisten.

- Programm-Module.

  Neben den Datenbanken von Kaspersky Internet Security können auch die Programm-Module aktualisiert werden. Updatepakete beheben Schwachstellen von Kaspersky Internet Security, fügen neue Funktionen hinzu und optimieren bestehende Funktionen.

Die wichtigste Updatequelle für Kaspersky Internet Security sind spezielle Updateserver von Kaspersky Lab.

Um die Updates von den Servern herunterzuladen, ist eine Verbindung Ihres Computers mit dem Internet erforderlich. In der Grundeinstellung wird die Internetverbindung automatisch ermittelt. Wenn die Proxyserver-Einstellungen nicht automatisch ermittelt werden, passen Sie die Parameter der Verbindung mit dem Proxyserver an.

Bei der Aktualisierung werden die Programm-Module und Datenbanken auf Ihrem Computer mit den auf der Updatequelle vorhandenen verglichen. Wenn auf Ihrem Computer die aktuelle Version der Datenbanken und Module installiert ist, erscheint auf dem Bildschirm eine Meldung darüber, dass der Schutz auf Ihrem Computer aktuell ist. Wenn Datenbanken und Module nicht aktuell sind, wird nur der fehlende Teil der Updates auf Ihrem Computer installiert. Datenbanken und Module werden nicht vollständig kopiert, wodurch die Updategeschwindigkeit wesentlich gesteigert und der Netzwerkverkehr entlastet wird.

Wenn die Datenbanken stark veraltet sind, kann das Updatepaket relativ umfangreich sein und zusätzlichen Internet-Datenverkehr verursachen (bis zu mehrere Dutzend MB).

Bevor die Datenbanken aktualisiert werden, legt Kaspersky Internet Security eine Sicherungskopie davon an. Bei Bedarf können Sie zur vorhergehenden Version der Datenbanken zurückkehren.

Die Option zum Rollback des Updates ist beispielsweise erforderlich, wenn Sie die Datenbanken aktualisiert haben und diese bei der Arbeit beschädigt wurden. Es ist möglich, zu der vorherigen Variante der Datenbanken zurückzukehren und die Aktualisierung später erneut zu versuchen.

Synchron zur Aktualisierung von Kaspersky Internet Security können Sie das Kopieren der heruntergeladenen Updates in eine lokale Quelle ausführen. Dieser Dienst erlaubt es, die Datenbanken und Module des Programms auf Netzwerkcomputern zu aktualisieren und dabei Netzwerkverkehr einzusparen.

Zusätzlich kann der Modus für den automatischen Start des Updates angepasst werden.

Im Abschnitt **Update** des Programmhauptfensters werden Informationen über den aktuellen Zustand der Datenbanken von Kaspersky Internet Security angezeigt:

- Datum und Uhrzeit des Erscheinens
- Anzahl und Zusammensetzung der Einträge in den Datenbanken.
- Status der Datenbanken (aktuell, veraltet oder beschädigt)

Sie können zum Bericht über das Update wechseln, der vollständige Informationen über die Ereignisse, die bei der Ausführung der Updateaufgabe eingetreten sind, bietet (der Link **Bericht** im oberen Bereich des Fensters). Außerdem können Sie auf der Seite www.kaspersky.com einen Überblick über die Virenaktivität erhalten (Link **Überblick über die Virenaktivität**).

IN DIESEM ABSCHNITT

Update starten 152

Rollback zum vorherigen Update 153

Updatequelle auswählen 153

Proxyserver verwenden 154

Regionsoptionen 154

Aktionen nach dem Update 154

Update aus einem lokalen Ordner 155

Startmodus für die Updateaufgabe ändern 156

Updatestart mit den Rechten eines anderen Benutzers 156

UPDATE STARTEN

Sie können das Update von Kaspersky Internet Security jederzeit starten. Es erfolgt aus der von Ihnen ausgewählten Updatequelle (s. Abschnitt "Updatequelle auswählen" auf S. 153).

Das Update von Kaspersky Internet Security kann auf zwei Arten gestartet werden:

- aus dem Kontextmenü (s. Abschnitt "Kontextmenü " auf S. 42).
- aus dem Hauptfenster (s. Abschnitt "Hauptfenster von Kaspersky Internet Security" auf S. 43).

Die Informationen über den Updateprozess werden im Abschnitt **Update** des Programmhauptfensters angezeigt.

Gehen Sie folgendermaßen vor, um das Update von Kaspersky Internet Security aus dem Kontextmenü zu starten:

1. Klicken Sie im Infobereich der Taskleiste mit der rechten Maustaste auf das Programmsymbol.
2. Wählen Sie im Kontextmenü den Punkt **Update** aus.

Gehen Sie folgendermaßen vor, um das Update aus dem Hauptfenster von Kaspersky Internet Security zu starten:

1. Öffnen Sie das Programmhauptfenster.
2. Wählen Sie auf der linken Fensterseite den Abschnitt **Update** aus.

3. Klicken Sie auf die Schaltfläche **Update ausführen**. Der Ausführungsfortschritt der Aufgabe wird im Programmhauptfenster dargestellt.

ROLLBACK ZUM VORHERIGEN UPDATE

Jedes Mal, wenn Sie das Update starten, erstellt Kaspersky Internet Security zuerst eine Sicherungskopie der bisher verwendeten Datenbanken und Programm-Module und beginnt danach mit der Aktualisierung. Dadurch wird Ihnen erlaubt, zur Verwendung der vorherigen Datenbanken zurückzukehren, wenn das Update erfolglos war.

Die Rollback-Funktion ist beispielsweise nützlich, wenn die Datenbanken teilweise beschädigt wurden. Lokale Datenbanken können entweder von einem Benutzer oder von einem bösartigen Programm beschädigt werden. Eine Beschädigung ist nur möglich, wenn der Selbstschutz (s. Abschnitt "Selbstschutz von Kaspersky Internet Security" auf S. 170) von Kaspersky Internet Security deaktiviert wurde. Sie können zu den vorherigen Datenbanken zurückkehren und die Aktualisierung später erneut versuchen.

➡ *Gehen Sie folgendermaßen vor, um zur Verwendung der vorhergehenden Version der Datenbanken zurückzukehren:*

1. Öffnen Sie das Programmhauptfenster.
2. Wählen Sie auf der linken Fensterseite den Abschnitt **Update** aus.
3. Klicken Sie auf die Schaltfläche **Rollback zu den vorherigen Datenbanken**.

UPDATEQUELLE AUSWÄHLEN

Eine *Updatequelle* ist eine Ressource, die Updates der Datenbanken und der Module für Kaspersky Internet Security enthält. Als Updatequelle können HTTP- oder FTP-Server, lokale Ordner oder Netzwerkordner dienen.

Als primäre Updatequelle gelten die Kaspersky-Lab-Updateserver. Dabei handelt es sich um spezielle Internetseiten, auf denen Updates der Datenbanken und Programm-Module für alle Kaspersky-Lab-Produkte zur Verfügung gestellt werden.

Updates, die sich auf einem Wechseldatenträger befinden, können Sie auf einer ftp- oder http-Seite oder in einem lokalen oder Netzwerkordner speichern.

Geben Sie zur Bestellung von Updates auf Wechseldatenträgern unbedingt an, ob Sie Updates für die Programm-Module erhalten möchten.

In der Grundeinstellung enthält die Liste nur die Kaspersky-Lab-Updateserver.

Wenn Sie als Updatequelle eine Ressource gewählt haben, die sich außerhalb des lokalen Netzwerks befindet, ist für die Aktualisierung eine Internetverbindung erforderlich.

Wenn mehrere Ressourcen als Updatequellen gewählt wurden, greift das Kaspersky Internet Security bei der Aktualisierung genau nach der Listenreihenfolge darauf zu und aktualisiert sich von der ersten verfügbaren Quelle.

➡ *Gehen Sie folgendermaßen vor, um eine Updatequelle auszuwählen:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
2. Wählen Sie auf der linken Fensterseite den Abschnitt **Update** aus.
3. Klicken Sie im Block **Updatequelle** auf die Schaltfläche **Einstellungen**.
4. Klicken Sie im folgenden Fenster auf der Registerkarte **Quelle** auf den Link **Hinzufügen**.

5. Wählen Sie im folgenden Fenster **Updatequelle auswählen** eine ftp- oder http-Seite oder geben Sie ihre IP-Adresse, den symbolischen Namen oder die URL-Adresse an.

PROXYSERVER VERWENDEN

Wenn die Internetverbindung über einen Proxyserver erfolgt, ist es erforderlich, die Parameter anzupassen.

Gehen Sie folgendermaßen vor, um die Proxyserver-Einstellungen anzupassen:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie auf der linken Fensterseite den Abschnitt **Update** aus.
3. Klicken Sie im Block **Updatequelle** auf die Schaltfläche **Einstellungen**.
4. Klicken Sie auf der Registerkarte **Quelle** auf die Schaltfläche **Proxyserver**.
5. Passen Sie im folgenden Fenster **Proxyserver-Einstellungen** die Parameter für den Proxyserver an.

REGIONSOPTIONEN

Wenn Sie die Kaspersky-Lab-Server als Updatequelle verwenden, kann der für Sie günstigste Standort des Servers für den Update-Download ausgewählt werden. Kaspersky Lab verfügt in mehreren Ländern der Erde über Server. Die Auswahl des geografisch am nächsten gelegenen Kaspersky-Lab-Updateservers kann die Dauer des Updates verkürzen und die Downloadgeschwindigkeit erhöhen.

Gehen Sie folgendermaßen vor, um den nächstliegenden Server auszuwählen:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie auf der linken Fensterseite den Abschnitt **Update** aus.
3. Klicken Sie im Block **Updatequelle** auf die Schaltfläche **Einstellungen**.
4. Aktivieren Sie im folgenden Fenster auf der Registerkarte **Quelle** im Block **Regionsoptionen** das Kontrollkästchen **Aus der Liste auswählen** und wählen Sie das Land aus, das sich am nächsten bei Ihrem Aufenthaltsort befindet.

   Wenn die Variante **Automatisch ermitteln** gewählt wurde, werden beim Update Informationen über den aktuellen Standort aus der Registrierung des Betriebssystems verwendet.

AKTIONEN NACH DEM UPDATE

In Kaspersky Internet Security können die Aktionen festgelegt werden, die automatisch nach dem Update ausgeführt werden sollen. Folgende Aktionen sind möglich:

- **Quarantänedateien untersuchen**. In die Quarantäne werden Objekte verschoben, bei deren Untersuchung nicht genau festgestellt werden konnte, von welchen schädlichen Programmen sie infiziert sind. Möglicherweise kann die Bedrohung eindeutig bestimmt und desinfiziert werden, nachdem die Datenbanken aktualisiert wurden. Deshalb untersucht das Programm die Quarantäneobjekte nach jedem Update. Es wird empfohlen, die Objekte in der Quarantäne regelmäßig zu überprüfen. Aufgrund der Untersuchung kann sich ihr Status ändern. Bestimmte Objekte können am ursprünglichen Ort wiederhergestellt und wieder verwendet werden.

- **Updates in folgenden Ordner kopieren**. Wenn Computer zu einem lokalen Netzwerk zusammengeschlossen sind, ist es überflüssig, die Updates für jeden Computer einzeln herunterzuladen und zu installieren, weil

dadurch eine erhöhte Netzwerkbelastung verursacht würde. Sie können die Funktion zur Update-Verteilung verwenden, mit dem der Netzwerkverkehr verringert werden kann, weil Updates nur einmal heruntergeladen werden müssen.

Gehen Sie folgendermaßen vor, damit die Dateien, die sich in der Quarantäne befinden, nach dem Update untersucht werden:

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
2. Wählen Sie auf der linken Fensterseite den Abschnitt **Update** aus.
3. Aktivieren Sie im Block **Erweitert** das Kontrollkästchen **Quarantänedateien nach jedem Update untersuchen**.

UPDATE AUS EINEM LOKALEN ORDNER

Die Update-Verteilung aus einem lokalen Ordner wird folgendermaßen organisiert:

1. Ein Computer des Netzwerks lädt das Paket mit den Updates für Kaspersky Internet Security von den Kaspersky-Lab-Webservern im Internet oder einer anderen Webressource, auf der sich die aktuellen Updates befinden, herunter. Die heruntergeladenen Updates werden in einem gemeinsamen Ordner abgelegt.
2. Die übrigen Netzwerkcomputer verwenden den gemeinsamen Ordner, um die Updates von Kaspersky Internet Security herunterzuladen.

Gehen Sie folgendermaßen vor, um den Modus für die Update-Verteilung zu aktivieren:

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
2. Wählen Sie auf der linken Fensterseite den Abschnitt **Update** aus.
3. Aktivieren Sie im Block **Erweitert** das Kontrollkästchen **Updates in folgenden Ordner kopieren** und geben Sie darunter im Feld den Pfad des gemeinsamen Ordners an, in dem die heruntergeladenen Updates abgelegt werden sollen. Der Pfad kann auch im Fenster, das mit der Schaltfläche **Durchsuchen** geöffnet wird, gewählt werden.

Damit das Update aus dem gewählten gemeinsamen Ordner erfolgt, nehmen Sie auf allen Computern des Netzwerks folgende Einstellungen vor:

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
2. Wählen Sie auf der linken Fensterseite den Abschnitt **Update** aus.
3. Klicken Sie im Block **Updatequelle** auf die Schaltfläche **Einstellungen**.
4. Klicken Sie im folgenden Fenster auf der Registerkarte **Quelle** auf den Link **Hinzufügen**.
5. Wählen Sie im folgenden Fenster **Updatequelle auswählen** den Ordner und geben Sie im Feld **Quelle** seinen vollständigen Pfad an.
6. Deaktivieren Sie auf der Registerkarte **Quelle** das Kontrollkästchen **Kaspersky-Lab-Updateserver**.

STARTMODUS FÜR DIE UPDATEAUFGABE ÄNDERN

Der Startmodus für das Update von Kaspersky Internet Security wird im Konfigurationsassistenten von Kaspersky Internet Security festgelegt (s. Abschnitt "Schritt 3. Programm-Update anpassen" auf S. 32) auswählen. Später kann der Startmodus für das Update geändert werden.

Für den Start der Updateaufgabe stehen folgende Modi zur Auswahl:

- **Automatisch**. Kaspersky Internet Security prüft in festgelegten Zeitabständen, ob an der Updatequelle ein Updatepaket vorhanden ist. Die Häufigkeit der Überprüfung kann während Viren-Epidemien steigen und unter gewöhnlichen Umständen sinken. Wenn neue Updates gefunden werden, lädt das Programm sie herunter und installiert sie auf dem Computer.
- **Nach Zeitplan** (Das Intervall ist von den Zeitplaneinstellungen abhängig). Das Update wird automatisch nach einem festgelegten Zeitplan gestartet.
- **Manuell**. In diesem Fall starten Sie das Update von Kaspersky Internet Security auf Befehl.

Gehen Sie folgendermaßen vor, um den Startmodus für die Updateaufgabe anzupassen:

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
2. Wählen Sie auf der linken Fensterseite den Abschnitt **Update** aus.
3. Klicken Sie im Block **Startmodus** auf die Schaltfläche **Einstellungen**.
4. Wählen Sie im folgenden Fenster auf der Registerkarte **Startmodus** im Block **Zeitplan** einen Startmodus für die Updateaufgabe. Wenn der Modus **Nach Zeitplan** gewählt wurde, legen Sie einen Zeitplan an.

   Wenn der Start einer Aufgabe aus einem bestimmten Grund übersprungen wurde (wenn beispielsweise der Computer ausgeschaltet war), können Sie festlegen, dass die übersprungene Aufgabe automatisch gestartet wird, sobald dies möglich ist. Aktivieren Sie dazu im unteren Bereich des Fensters das Kontrollkästchen **Übersprungene Aufgaben starten**. Dieses Kontrollkästchen steht für alle Zeitplanvarianten zur Verfügung, außer für **Stunden**, **Minuten** und **Nach dem Programmstart**.

UPDATESTART MIT DEN RECHTEN EINES ANDEREN BENUTZERS

Das Update wird standardmäßig unter dem Benutzerkonto gestartet, mit dessen Rechten Sie sich im System angemeldet haben. Das Update für Kaspersky Internet Security kann aber aus einer Quelle (z.B. Netzwerkordner, der Updates enthält) erfolgen, auf die Sie keinen Zugriff besitzen oder für die Sie nicht über Rechte eines autorisierten Benutzers für den Proxyserver verfügen. Sie können das Update von Kaspersky Internet Security unter dem Namen eines Benutzers starten, der über die erforderlichen Privilegien verfügt.

Gehen Sie folgendermaßen vor, um das Update mit den Rechten eines anderen Benutzers zu starten:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie auf der linken Fensterseite den Abschnitt **Update** aus.
3. Klicken Sie im Block **Startmodus** auf die Schaltfläche **Einstellungen**.
4. Aktivieren Sie im folgenden Fenster auf der Registerkarte **Startmodus** im Block **Benutzer** das Kontrollkästchen **Aufgabe starten mit Rechten des anderen Benutzers**. Geben Sie darunter in den Feldern den Benutzernamen und das Kennwort an.

PROGRAMMPARAMETER ANPASSEN

Das Programmkonfigurationsfenster dient dem schnellen Zugriff auf die wichtigsten Einstellungen von Kaspersky Internet Security.

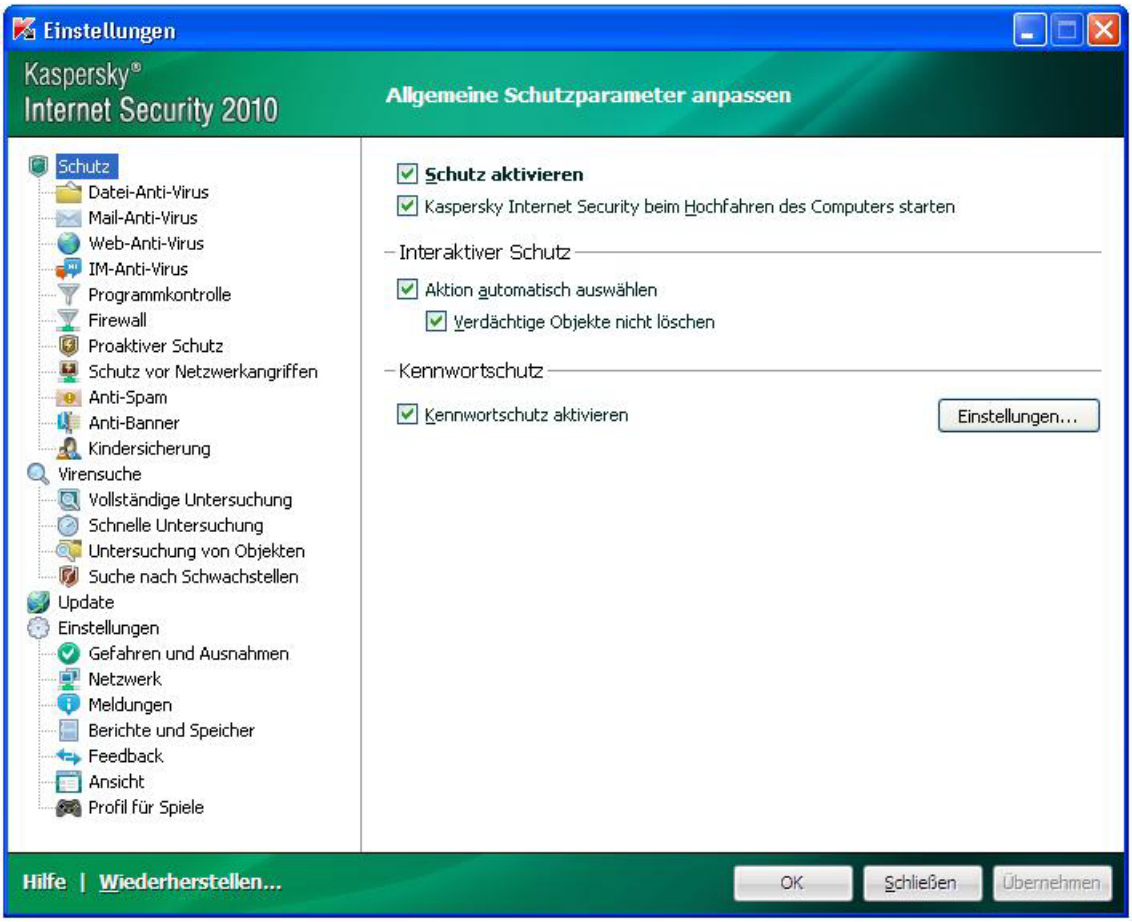

Abbildung 11: Konfigurationsfenster für Programmeinstellungen

Das Konfigurationsfenster besteht aus zwei Teilen:

- Die linke Seite des Fensters bietet Zugriff auf die Komponenten von Kaspersky Internet Security, auf Untersuchungs- und Updateaufgaben und andere Funktionen.

- Die rechte Seite des Fensters enthält eine Liste von Parametern für die auf der linken Seite ausgewählte Komponente, Aufgabe usw.

Zum Öffnen des Fensters gibt es folgende Möglichkeiten:

- aus dem Hauptfenster (s. Abschnitt "Hauptfenster von Kaspersky Internet Security" auf S. 43) von Kaspersky Internet Security. Klicken Sie dazu im oberen Bereich des Hauptfensters auf den Link **Einstellungen**.

- aus dem Kontextmenü (s. Abschnitt "Kontextmenü " auf S. 42). Wählen Sie dazu im Kontextmenü des Programms den Punkt **Einstellungen** aus.

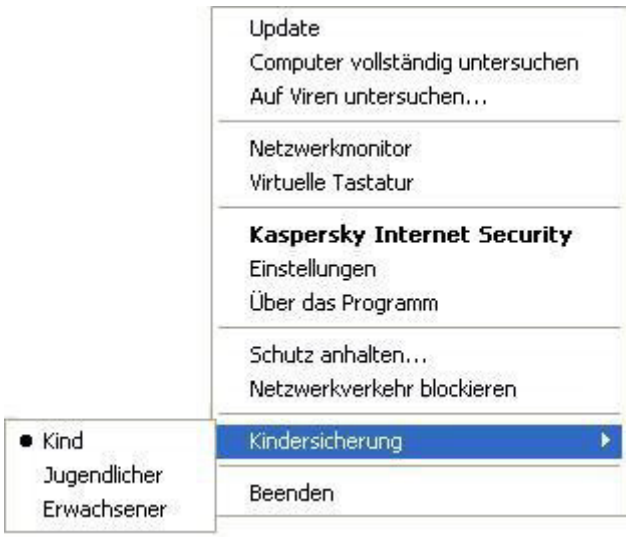

Abbildung 12: Kontextmenü

IN DIESEM ABSCHNITT

Schutz 159

Datei-Anti-Virus 161

Mail-Anti-Virus 161

Web-Anti-Virus 162

IM-Anti-Virus 163

Programmkontrolle 163

Firewall 164

Proaktiver Schutz 165

Schutz vor Netzwerkangriffen 165

Anti-Spam 166

Anti-Banner 167

Kindersicherung 168

Untersuchung 169

Update 170

Einstellungen 170

SCHUTZ

Im Fenster **Schutz** können Sie folgende Zusatzfunktionen von Kaspersky Internet Security verwenden:

- Schutz von Kaspersky Internet Security aktivieren / deaktivieren (s. S. 159).
- Kaspersky Internet Security beim Hochfahren des Betriebssystems starten (s. S. 159).
- Interaktiven Schutzmodus verwenden (s. S. 160).
- Kontrolle des Zugriffs auf Kaspersky Internet Security (s. S. 160).

COMPUTERSCHUTZ AKTIVIEREN / DEAKTIVIEREN

Kaspersky Internet Security wird in der Grundeinstellung automatisch beim Start des Betriebssystems gestartet und schützt Ihren Computer während der gesamten Sitzung. Alle Schutzkomponenten sind aktiv.

Sie können den Schutz, der von Kaspersky Internet Security gewährleistet wird, vollständig oder teilweise deaktivieren.

Die Kaspersky-Lab-Spezialisten **warnen ausdrücklich davor, den Schutz zu deaktivieren**, weil dies zur Infektion Ihres Computers und zu Datenverlust führen kann.

Wenn der Schutz deaktiviert wird, wird die Arbeit aller Komponenten beendet. Darüber informieren folgende Merkmale:

- Das inaktive (graue) Symbol von Kaspersky Internet Security (s. Abschnitt "Symbol im Infobereich der Taskleiste" auf S. 41) im Infobereich der Taskleiste.
- Die rote Farbe des Sicherheitsindikators.

Beachten Sie, dass der Schutz hier ausdrücklich im Kontext der Schutzkomponenten beschrieben wird. Das Deaktivieren oder Anhalten von Schutzkomponenten übt keinen Einfluss auf die Ausführung von Aufgaben zur Virensuche und zum Update für Kaspersky Internet Security aus.

➧ *Gehen Sie folgendermaßen vor, um den Schutz vollständig auszuschalten:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
2. Wählen Sie im folgenden Fenster den Abschnitt **Schutz**.
3. Deaktivieren Sie das Kontrollkästchen **Schutz aktivieren**.

KASPERSKY INTERNET SECURITY BEIM HOCHFAHREN DES BETRIEBSSYSTEMS STARTEN

Wenn es erforderlich ist, die Arbeit von Kaspersky Internet Security vollständig zu beenden, wählen Sie im Kontextmenü (s. Abschnitt "Kontextmenü" auf S. 42) von Kaspersky Internet Security den Punkt **Beenden** aus. Dadurch wird das Programm aus dem Arbeitsspeicher entfernt. Das bedeutet, Ihr Computer ist ungeschützt.

Der Computerschutz kann wieder aktiviert werden, indem Kaspersky Internet Security aus dem **Startmenü** → **Programme** → **Kaspersky Internet Security 2010** → **Kaspersky Internet Security 2010** gestartet wird.

Außerdem kann der Schutz nach dem Neustart des Betriebssystems automatisch gestartet werden.

Gehen Sie folgendermaßen vor, um diesen Modus zu aktivieren:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie im folgenden Fenster den Abschnitt **Schutz**.
3. Aktivieren Sie das Kontrollkästchen **Kaspersky Internet Security beim Hochfahren des Computers starten**.

INTERAKTIVEN SCHUTZMODUS VERWENDEN

Kaspersky Internet Security bietet zwei Modi für die Kooperation mit dem Benutzer:

- *Interaktiver Schutzmodus*. Kaspersky Internet Security benachrichtigt den Benutzer über alle gefährlichen und verdächtigen Ereignisse im System. In diesem Modus muss der Benutzer selbständig entscheiden, ob bestimmte Aktionen erlaubt oder verboten werden sollen.
- *Automatischer Schutzmodus*. Kaspersky Internet Security führt automatisch die von den Kaspersky-Lab-Experten empfohlene Aktion aus, wenn gefährliche Ereignisse eintreten.

Gehen Sie folgendermaßen vor, um den automatischen Schutzmodus zu verwenden:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie im folgenden Fenster den Abschnitt **Schutz**.
3. Aktivieren Sie im Block **Interaktiver Schutz** das Kontrollkästchen **Aktion automatisch auswählen**. Wenn verdächtige Objekte bei der Arbeit im automatischen Modus nicht gelöscht werden sollen, dann aktivieren Sie das Kontrollkästchen **Verdächtige Objekte nicht löschen**.

KONTROLLE DES ZUGRIFFS AUF KASPERSKY INTERNET SECURITY

Es kann sein, dass ein PC von mehreren Benutzern verwendet wird, deren Fertigkeiten im Umgang mit Computern völlig unterschiedlich sind. Der ungehinderte Zugriff auf Kaspersky Internet Security und dessen Einstellungen kann das Sicherheitsniveau des Computers stark einschränken.

Verwenden Sie ein Kennwort für den Zugriff auf Kaspersky Internet Security, um die Sicherheit des Computers zu erhöhen. Sie können entweder alle Operationen mit Kaspersky Internet Security blockieren (unter Ausnahme der Arbeit mit Meldungen über den Fund gefährlicher Objekte) oder das Ausführen folgender Aktionen untersagen:

- Programmparameter ändern.
- Programm beenden.

Gehen Sie folgendermaßen vor, um den Zugriff auf Kaspersky Internet Security durch ein Kennwort zu schützen:

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
2. Wählen Sie im folgenden Fenster den Abschnitt **Schutz**.
3. Aktivieren Sie im Block **Kennwortschutz** das Kontrollkästchen **Kennwortschutz aktivieren** und klicken Sie auf die Schaltfläche **Einstellungen**.
4. Geben Sie im folgenden Fenster **Kennwortschutz** das Kennwort an und legen Sie den Bereich fest, für den die Zugriffsbeschränkung gelten soll. Beim Versuch eines beliebigen Benutzers Ihres Computers, die von Ihnen festgelegten Aktionen auszuführen, wird Kaspersky Internet Security nun immer das Kennwort abfragen.

DATEI-ANTI-VIRUS

Im Fenster sind die Parameter für die Komponente Datei-Anti-Virus (s. Abschnitt "Schutz für das Dateisystem des Computers" auf S. 47) angeordnet. Durch eine Veränderung der Parameterwerte, können Sie folgende Aktionen ausführen:

- Datei-Anti-Virus deaktivieren.
- Sicherheitsstufe ändern (s. S. 49).
- Aktion für erkannte Objekte ändern (s. S. 49).
- Schutzbereich festlegen (s. S. 50).
- Untersuchung optimieren (s. S. 52).
- Untersuchung von zusammengesetzten Dateien anpassen (s. S. 52).
- Untersuchungsmodus ändern (s. S. 53).
- heuristische Analyse verwenden (s. S. 51).
- Komponente anhalten (s. S. 54).
- Untersuchungstechnologie auswählen (s. S. 53).
- Standard-Schutzeinstellungen wiederherstellen (s. S. 56), wenn sie geändert wurden.

Gehen Sie folgendermaßen vor, um Datei-Anti-Virus zu deaktivieren:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Datei-Anti-Virus** aus.
3. Deaktivieren Sie auf der rechten Fensterseite das Kontrollkästchen **Datei-Anti-Virus aktivieren**.

Gehen Sie folgendermaßen vor, um zu den Einstellungen für Datei-Anti-Virus zu gelangen:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Datei-Anti-Virus** aus.
3. Wählen Sie auf der rechten Fensterseite die Sicherheitsstufe und die Reaktion der Komponente auf die Bedrohung aus. Klicken Sie auf die Schaltfläche **Einstellungen**, um andere Parameter von Datei-Anti-Virus anzupassen.

MAIL-ANTI-VIRUS

Im Fenster sind die Parameter für die Komponente Mail-Anti-Virus (s. Abschnitt "E-Mail-Schutz" auf S. 57) angeordnet. Durch eine Veränderung der Parameterwerte, können Sie folgende Aktionen ausführen:

- Mail-Anti-Virus deaktivieren.
- Sicherheitsstufe ändern (s. S. 58).
- Aktion für erkannte Objekte ändern (s. S. 59).

- Schutzbereich festlegen (s. S. 60).
- heuristische Analyse verwenden (s. S. 62).
- Untersuchung von zusammengesetzten Dateien anpassen (s. S. 62).
- Filterbedingungen für an E-Mails angehängte Objekte anpassen. (s. S. 62).
- Standard-Schutzeinstellungen wiederherstellen (s. S. 63).

Gehen Sie folgendermaßen vor, um Mail-Anti-Virus zu deaktivieren:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Mail-Anti-Virus** aus.
3. Deaktivieren Sie auf der rechten Fensterseite das Kontrollkästchen **Mail-Anti-Virus aktivieren**.

Gehen Sie folgendermaßen vor, um zu den Einstellungen für Mail-Anti-Virus zu gelangen:

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Mail-Anti-Virus** aus.
3. Wählen Sie auf der rechten Fensterseite die Sicherheitsstufe und die Reaktion der Komponente auf die Bedrohung aus. Klicken Sie auf die Schaltfläche **Einstellungen**, um andere Parameter von Mail-Anti-Virus anzupassen.

WEB-ANTI-VIRUS

Im Fenster sind die Parameter für die Komponente Web-Anti-Virus (s. Abschnitt "Schutz für Web-Datenverkehr" auf S. 64) angeordnet. Durch eine Veränderung der Parameterwerte, können Sie folgende Aktionen ausführen:

- Web-Anti-Virus deaktivieren.
- Sicherheitsstufe ändern (s. S. 66).
- Aktion für erkannte Objekte ändern (s. S. 66).
- Schutzbereich festlegen (s. S. 67).
- Untersuchungsmethoden ändern (s. S. 67).
- Modul für Link-Untersuchung verwenden (s. S. 68).
- Untersuchung optimieren (s. S. 69).
- heuristische Analyse verwenden (s. S. 69).
- Standardparameter für den Web-Schutz wiederherstellen (s. S. 70).

Gehen Sie folgendermaßen vor, um Web-Anti-Virus zu deaktivieren:

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Web-Anti-Virus** aus.

3. Deaktivieren Sie auf der rechten Seite des Fensters das Kontrollkästchen **Web-Anti-Virus aktivieren**.

Gehen Sie folgendermaßen vor, um zu den Einstellungen für Web-Anti-Virus zu gelangen:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.

2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Web-Anti-Virus** aus.

3. Wählen Sie auf der rechten Fensterseite die Sicherheitsstufe und die Reaktion der Komponente auf die Bedrohung aus. Klicken Sie auf die Schaltfläche **Einstellungen**, um andere Parameter von Web-Anti-Virus anzupassen.

IM-ANTI-VIRUS

Im Fenster sind die Parameter für die Komponente IM-Anti-Virus (s. Abschnitt "Schutz für den Datenverkehr von Instant-Messengern" auf S. 71) angeordnet. Durch eine Veränderung der Parameterwerte, können Sie folgende Aktionen ausführen:

- IM-Anti-Virus deaktivieren.
- Schutzbereich festlegen (s. S. 72).
- Untersuchungsmethode ändern (s. S. 72).
- heuristische Analyse verwenden (s. S. 73).

Gehen Sie folgendermaßen vor, um IM-Anti-Virus zu deaktivieren:

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.

2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **IM-Anti-Virus** aus.

3. Deaktivieren Sie auf der rechten Seite des Fensters das Kontrollkästchen **IM-Anti-Virus aktivieren**.

Gehen Sie folgendermaßen vor, um zu den Einstellungen für IM-Anti-Virus zu gelangen:

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.

2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **IM-Anti-Virus** aus.

3. Passen Sie die Parameter der Komponente auf der rechten Seite des Fensters entsprechend an.

PROGRAMMKONTROLLE

Dieses Fenster enthält die Parameter der Komponente Programmkontrolle (auf S. 74). Durch eine Veränderung der Parameterwerte, können Sie folgende Aktionen ausführen:

- Programmkontrolle deaktivieren.
- Schutzbereich festlegen (s. S. 77).
- Verteilung von Programmen auf Gruppen verwalten (s. S. 80).
- Dauer der Statusermittlung für ein Programm ändern (s. S. 80).

- Regel für ein Programm ändern (s. S. 81).
- Regel für eine Programmgruppe ändern (s. S. 81).
- Netzwerkregel für ein Programm erstellen (s. S. 82).
- Ausnahmen festlegen (s. S. 82).
- Löschen von Regeln für Programme verwalten (s. S. 83).

Gehen Sie folgendermaßen vor, um die Programmkontrolle zu deaktivieren:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Programmkontrolle** aus.
3. Deaktivieren Sie auf der rechten Seite des Fensters das Kontrollkästchen **Programmkontrolle aktivieren**.

Gehen Sie folgendermaßen vor, um zu den Einstellungen für die Programmkontrolle zu gelangen:

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Programmkontrolle** aus.
3. Passen Sie die Parameter der Komponente auf der rechten Seite des Fensters entsprechend an.

FIREWALL

Dieses Fenster enthält die Parameter der Komponente Firewall (auf S. 89). Durch eine Veränderung der Parameterwerte, können Sie folgende Aktionen ausführen:

- Firewall deaktivieren.
- Netzwerkstatus ändern (s. S. 89).
- Adressenbereich eines Netzwerks erweitern (s. S. 90).
- Modus für die Benachrichtigung über Veränderungen eines Netzwerks auswählen (s. S. 91).
- Erweiterte Einstellungen für die Komponente festlegen (s. S. 91).
- Firewall-Regeln erstellen (s. S. 92).
  - Paketregel erstellen (s. S. 92).
  - Netzwerkregel für ein Programm erstellen (s. S. 93).
  - Assistent für neue Regeln verwenden (s. S. 94).
  - Aktion auswählen, die von einer Regel ausgeführt werden soll (s. S. 94).
  - Parameter eines Netzwerkdiensts anpassen (s. S. 95).
  - Adressenbereich auswählen (s. S. 95).
  - Priorität einer Regel ändern.

Gehen Sie folgendermaßen vor, um die Firewall zu deaktivieren:

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Firewall** aus.
3. Deaktivieren Sie auf der rechten Seite des Fensters das Kontrollkästchen **Firewall aktivieren**.

Gehen Sie folgendermaßen vor, um zu den Einstellungen für Firewall zu gelangen:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Firewall** aus.
3. Klicken Sie auf der rechten Seite des Fensters auf die Schaltfläche **Einstellungen** und passen Sie die Parameter der Komponente im folgenden Fenster entsprechend an.

PROAKTIVER SCHUTZ

Dieses Fenster enthält die Parameter der Komponente Proaktiver Schutz (auf S. 97). Durch eine Veränderung der Parameterwerte, können Sie folgende Aktionen ausführen:

- Proaktiven Schutz deaktivieren.
- Liste der gefährlichen Aktivitäten verwalten (s. S. 97).
- Reaktion des Programms auf gefährliche Aktivität im System ändern (s. S. 98).
- Gruppe mit vertrauenswürdigen Programmen erstellen (s. S. 99).
- System-Benutzerkonten kontrollieren (s. S. 99).

Gehen Sie folgendermaßen vor, um den Proaktiven Schutz zu deaktivieren:

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Proaktiver Schutz** aus.
3. Deaktivieren Sie auf der rechten Seite des Fensters das Kontrollkästchen **Proaktiven Schutz aktivieren**.

Gehen Sie folgendermaßen vor, um zu den Einstellungen für den Proaktiven Schutz zu gelangen:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Proaktiver Schutz** aus.
3. Passen Sie die Parameter der Komponente auf der rechten Seite des Fensters entsprechend an.

SCHUTZ VOR NETZWERKANGRIFFEN

Dieses Fenster enthält die Parameter der Komponente Schutz vor Netzwerkangriffen (auf S. 100). Durch eine Veränderung der Parameterwerte, können Sie folgende Aktionen ausführen:

- Schutz vor Netzwerkangriffen deaktivieren.

- Angreifenden Computer zur Sperrliste hinzufügen (s. S. 100).

Gehen Sie folgendermaßen vor, um den Schutz vor Netzwerkangriffen zu deaktivieren:

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Schutz vor Netzwerkangriffen** aus.
3. Deaktivieren Sie auf der rechten Seite des Fensters das Kontrollkästchen **Schutz vor Netzwerkangriffen aktivieren**.

Gehen Sie folgendermaßen vor, um zu den Einstellungen für den Schutz vor Netzwerkangriffen zu gelangen:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Schutz vor Netzwerkangriffen** aus.
3. Passen Sie die Parameter der Komponente auf der rechten Seite des Fensters entsprechend an.

ANTI-SPAM

Dieses Fenster enthält die Parameter der Komponente Anti-Spam (auf S. 103). Durch eine Veränderung der Parameterwerte, können Sie folgende Aktionen ausführen:

- Anti-Spam deaktivieren.
- Anti-Spam trainieren (s. S. 106):
  - mit Hilfe des Trainingsassistenten (s. S. 106).
  - mit ausgehenden E-Mails (s. S. 107).
  - mit Hilfe eines Mailprogramms (s. S. 108).
  - mit Hilfe von Berichten (s. S. 109).
- Sicherheitsstufe ändern (s. S. 109).
- Untersuchungsmethode ändern (s. S. 110).
- Liste erstellen:
  - für vertrauenswürdige Adressen (s. S. 111).
  - für verbotene Absender (s. S. 111).
  - für verbotene Phrasen (s. S. 112).
  - für anstößige Phrasen (s. S. 112).
  - für erlaubte Absender (s. S. 113).
  - für erlaubte Phrasen (s. S. 114).
- Liste mit erlaubten Absendern importieren (s. S. 114).
- Faktoren für Spam und potentiellen Spam festlegen (s. S. 115).

- Algorithmus zur Spam-Erkennung auswählen (s. S. 116).
- zusätzliche Merkmale für die Spam-Filterung verwenden (s. S. 116).
- Markierung zum Betreff einer Nachricht hinzufügen (s. S. 117).
- Mail-Manager verwenden (s. S. 117).
- Nachrichten für Microsoft Exchange Server von der Untersuchung ausschließen (s. S. 118).
- Spam-Verarbeitung anpassen:
  - in Microsoft Office Outlook (s. S. 119).
  - in Microsoft Outlook Express (Windows Mail) (s. S. 120).
  - in The Bat! (s. S. 121).
  - in Thunderbird (s. S. 122).
- standardmäßige Parameter für den Schutz vor unerwünschten E-Mails wiederherzustellen (s. S. 122).

Gehen Sie folgendermaßen vor, um Anti-Spam zu deaktivieren:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Anti-Spam** aus.
3. Deaktivieren Sie auf der rechten Fensterseite das Kontrollkästchen **Anti-Spam aktivieren**.

Gehen Sie folgendermaßen vor, um zu den Einstellungen für Anti-Spam zu gelangen:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Anti-Spam** aus.
3. Klicken Sie auf der rechten Seite des Fensters auf die Schaltfläche **Einstellungen** und passen Sie die Parameter der Komponente im folgenden Fenster entsprechend an.

ANTI-BANNER

Dieses Fenster enthält die Parameter der Komponente Anti-Banner (auf S. 123). Durch eine Veränderung der Parameterwerte, können Sie folgende Aktionen ausführen:

- Anti-Banner deaktivieren.
- heuristische Analyse verwenden (s. S. 123).
- Erweiterte Einstellungen für die Komponente festlegen (s. S. 124).
- Liste der erlaubten Adressen erstellen (s. S. 124).
- Liste der verbotenen Adressen erstellen (s. S. 125).
- Bannerlisten exportieren / importieren (s. S. 125).

Gehen Sie folgendermaßen vor, um Anti-Banner zu deaktivieren:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Anti-Banner** aus.
3. Deaktivieren Sie auf der rechten Fensterseite das Kontrollkästchen **Anti-Banner aktivieren**.

Gehen Sie folgendermaßen vor, um zu den Einstellungen für Anti-Banner zu gelangen:

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Anti-Banner** aus.
3. Passen Sie die Parameter der Komponente auf der rechten Seite des Fensters entsprechend an.

KINDERSICHERUNG

Dieses Fenster enthält die Parameter der Komponente Kindersicherung (auf S. 126). Durch eine Veränderung der Parameterwerte, können Sie folgende Aktionen ausführen:

- Kindersicherung deaktivieren.
- Arbeit mit Profilen verwalten (s. S. 128).
- Beschränkungsstufe ändern (s. S. 129).
- Anzeige von Webressourcen beschränken (s. S. 130).
- Liste mit erlaubten Webadressen erstellen (s. S. 130).
- Liste mit verbotenen Webadressen erstellen (s. S. 132).
- Liste mit Webadressen exportieren / importieren (s. S. 132).
- Kategorien für verbotene Webadressen auswählen (s. S. 133).
- heuristische Analyse verwenden (s. S. 134).
- Aktion bei einem Zugriffsversuch auf verbotene Webadressen auswählen (s. S. 134).
- Zugriff zeitlich beschränken (s. S. 134).

Gehen Sie folgendermaßen vor, um die Kindersicherung zu deaktivieren:

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Kindersicherung** aus.
3. Deaktivieren Sie auf der rechten Seite des Fensters das Kontrollkästchen **Kindersicherung aktivieren**.

Gehen Sie folgendermaßen vor, um zu den Einstellungen für die Kindersicherung zu gelangen:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Kindersicherung** aus.

3. Klicken Sie auf der rechten Seite des Fensters auf die Schaltfläche **Einstellungen** und passen Sie die Parameter der Komponente im folgenden Fenster entsprechend an.

UNTERSUCHUNG

Auf welche Weise die Untersuchung von Objekten auf Ihrem Computer erfolgt, wird durch eine Auswahl von Parametern bestimmt, die für jede Aufgabe festgelegt werden.

Die Spezialisten von Kaspersky Lab haben Aufgaben für die Virensuche und für die Suche nach Schwachstellen vordefiniert. Zu den Aufgaben für die Virensuche gehören:

- **Objekte untersuchen**. Untersuchung von Objekten, die der Benutzer festlegt. Sie können ein beliebiges Objekt des Dateisystems auf dem Computer untersuchen.
- **Vollständige Untersuchung**. Ausführliche Untersuchung des Systems. Standardmäßig werden folgende Objekte untersucht: Systemspeicher, Objekte, die beim Systemstart gestartet werden, Systemwiederherstellung, Mail-Datenbanken, Festplatten, Wechseldatenträger und Netzlaufwerke.
- **Schnelle Untersuchung**. Virenuntersuchung der Objekte, die beim Start des Betriebssystems geladen werden.

Im Konfigurationsfenster können Sie für jede Untersuchungsaufgabe folgende Aktionen ausführen:

- Sicherheitsstufe auswählen, auf deren Basis die Aufgabe ausgeführt werden soll.
- Aktion auswählen, die vom Programm beim Fund eines infizierten bzw. möglicherweise infizierten Objekts angewandt wird.
- Zeitplan für den automatischen Aufgabenstart erstellen.
- Liste der Untersuchungsobjekte erstellen (für die Aufgaben zur schnellen und vollständigen Untersuchung).
- Typen der Dateien, die der Virenanalyse unterzogen werden, festlegen.
- Parameter für die Untersuchung von zusammengesetzten Dateien festlegen.
- Methoden und Technologien für die Untersuchung auswählen.

Im Abschnitt **Untersuchung** lassen sich die Parameter für die automatische Untersuchung von Wechseldatenträgern bei deren Verbindung mit dem Computer angeben und Verknüpfungen für einen schnellen Start der Aufgaben Virenuntersuchung und Schwachstellensuche herstellen.

Im Konfigurationsfenster der Aufgabe zur Schwachstellen-Suche können Sie:

- Zeitplan für den automatischen Aufgabenstart erstellen.
- Liste der Untersuchungsobjekte erstellen.

Gehen Sie folgendermaßen vor, um die Aufgabenparameter anzupassen:

1. Öffnen Sie das Programmhauptfenster.
2. Wählen Sie auf der linken Seite des Fensters im Abschnitt **Untersuchung** die erforderliche Aufgabe aus (**Vollständige Untersuchung**, **Schnelle Untersuchung**, **Untersuchung von Objekten**, **Suche nach Schwachstellen**).
3. Nehmen Sie auf der rechten Seite des Fensters die entsprechenden Einstellungen vor.

UPDATE

Das Update von Kaspersky Internet Security wird nach den folgenden Parametern ausgeführt:

Im Konfigurationsfenster für die Updateaufgabe können Sie folgende Aktionen ausführen:

- Adresse der Quelle ändern, von der die Updates des Programms kopiert und installiert werden.
- Den Modus bestimmen, in dem der Updateprozess für das Programm gestartet wird.
- Zeitplan für Start der Aufgabe erstellen.
- Benutzerkonto, in dessen Namen das Update gestartet wird, angeben.
- Aktionen, die nach dem Programm-Update ausgeführt werden sollen, angeben.

Gehen Sie folgendermaßen vor, um zur Konfiguration der Updateparameter zu wechseln:

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
2. Wählen Sie auf der linken Fensterseite den Abschnitt **Update** aus.
3. Wählen Sie auf der rechten Seite des Fensters den erforderlichen Startmodus aus. Geben Sie im Block **Erweitert** weitere Aufgabenparameter an.

EINSTELLUNGEN

Im Fenster **Einstellungen** können Sie folgende Zusatzfunktionen von Kaspersky Internet Security verwenden:

- Selbstschutz für Kaspersky Internet Security (s. S. 170).
- Technologie der aktiven Desinfektion verwenden (s. S. 171).
- Dienst zum Sparen von Akkustrom (s. S. 171).
- Zurückgestellte Ausführung von Aufgaben zur Virensuche bei verlangsamter Arbeit anderer Programme (s. S. 172).
- Funktionsparameter für Kaspersky Internet Security exportieren / importieren (s. S. 172).
- Standardmäßige Funktionsparameter für Kaspersky Internet Security wiederherstellen (s. S. 173).

SELBSTSCHUTZ FÜR KASPERSKY INTERNET SECURITY

Kaspersky Internet Security bietet dem Computer Sicherheit vor schädlichen Programmen und wird dadurch selbst zu einem Objekt von Schädlingen, die versuchen können, die Arbeit des Programms zu blockieren oder es sogar vom Computer zu löschen.

Um die Stabilität des Sicherheitssystems für Ihren Computer zu gewährleisten, verfügt Kaspersky Internet Security über Mechanismen zum Selbstschutz und zum Schutz vor externem Zugriff.

Für 64-Bit-Betriebssysteme und für Microsoft Windows Vista steht der Selbstschutzmechanismus von Kaspersky Internet Security nur im Hinblick auf Veränderungen oder Löschen von Dateien auf der Festplatte, sowie von Einträgen in der Systemregistrierung zur Verfügung.

Wenn der Schutz vor Fernsteuerung aktiviert ist, kann es vorkommen, dass gleichzeitig Programme, die der Remote-Administration dienen, eingesetzt werden sollen (z.B. RemoteAdmin). Um die Arbeit mit ihnen zu ermöglichen, werden diese Programme zur Liste der vertrauenswürdigen Programme hinzugefügt und der Parameter **Programmaktivität nicht kontrollieren** wird für sie aktiviert.

Gehen Sie folgendermaßen vor, um die Selbstschutzmechanismen für Kaspersky Internet Security zu aktivieren:

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.

2. Wählen Sie im folgenden Fenster den Abschnitt **Einstellungen**.

3. Aktivieren Sie im Block **Selbstschutz** das Kontrollkästchen **Selbstschutz aktivieren**, damit der Mechanismus zum Schutz von Kaspersky Internet Security vor dem Verändern oder Löschen von eigenen Dateien auf der Festplatte, Prozessen im Arbeitsspeicher und Einträgen in der Systemregistrierung wirksam wird.

   Aktivieren Sie im Block **Selbstschutz** das Kontrollkästchen **Option zur externen Steuerung des Systemdiensts deaktivieren**, um alle Versuche zur Fernsteuerung eines Anwendungsdiensts zu blockieren.

   Wird versucht, eine der oben genannten Aktionen auszuführen, dann erscheint eine Meldung über dem Programmsymbol im Infobereich der Taskleiste (falls der Benachrichtigungsdienst nicht vom Benutzer deaktiviert wurde).

TECHNOLOGIE ZUR DESINFEKTION EINER AKTIVEN INFEKTION

Moderne Schadprogramme können in die tiefste Ebene des Betriebssystems eindringen, wodurch es praktisch unmöglich wird, sie zu löschen. Wenn Kaspersky Internet Security eine schädliche Aktivität im System erkennt, bietet er an, einen speziell dafür vorgesehenen erweiterten Desinfektionsvorgang auszuführen, durch den die Bedrohung neutralisiert und vom Computer gelöscht wird.

Zum Abschluss des Vorgangs erfolgt ein obligatorischer Neustart des Computers. Nach dem Neustart des Computers wird empfohlen, die vollständige Virenuntersuchung zu starten.

Gehen Sie folgendermaßen vor, um die Prozedur zur erweiterten Desinfektion zu aktivieren:

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.

2. Wählen Sie im folgenden Fenster den Abschnitt **Einstellungen**.

3. Aktivieren Sie im Block **Kompatibilität** das Kontrollkästchen **Technologie zur aktiven Desinfektion verwenden**.

ARBEIT VON KASPERSKY INTERNET SECURITY AUF EINEM LAPTOP

Um sparsam mit der Batterie eines Laptops umzugehen, können Sie Untersuchungsaufgaben aufschieben.

Da die Virenuntersuchung und die Aktualisierung relativ viel Ressourcen und Zeit benötigen, empfehlen wir Ihnen, den zeitgesteuerten Start solcher Aufgaben zu deaktivieren. Dadurch können Sie Akkustrom sparen. Bei Bedarf können Sie Kaspersky Internet Security auf Befehl aktualisieren oder die Virenuntersuchung manuell starten.

Gehen Sie folgendermaßen vor, um den Dienst zum Stromsparen im Akkubetrieb zu verwenden:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.

2. Wählen Sie im folgenden Fenster den Abschnitt **Einstellungen**.

3. Aktivieren Sie im Block **Kompatibilität** das Kontrollkästchen **Geplante Untersuchungsaufgaben bei Akkubetrieb nicht starten**.

LEISTUNG DES COMPUTERS BEIM AUSFÜHREN VON AUFGABEN

Um die Belastung des Prozessors und der Laufwerkssubsysteme zu reduzieren, können Sie festlegen, dass Aufgaben zur Virensuche aufgeschoben werden.

Das Ausführen von Untersuchungsaufgaben erhöht die Auslastung des Prozessors und der Laufwerkssubsysteme und verlangsamt dadurch die Arbeit anderer Programme. In der Grundeinstellung hält Kaspersky Internet Security beim Eintreten dieser Situation die Ausführung von Untersuchungsaufgaben an und gibt Systemressourcen für Benutzeranwendungen frei.

Allerdings existiert eine Reihe von Programmen, die gestartet werden, wenn Prozessorressourcen frei werden, und im Hintergrundmodus arbeiten. Wenn die Untersuchung von der Arbeit solcher Programme unabhängig sein soll, sollten ihnen keine Systemressourcen überlassen werden.

Beachten Sie, dass dieser Parameter für jede Untersuchungsaufgabe individuell angepasst werden kann. In diesem Fall besitzt der für eine konkrete Aufgabe festgelegte Parameter die höchste Priorität.

- *Gehen Sie folgendermaßen vor, damit Untersuchungsaufgaben zurückgestellt werden, wenn sie die Arbeit anderer Programme verlangsamen:*

  1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.

  2. Wählen Sie im folgenden Fenster den Abschnitt **Einstellungen**.

  3. Aktivieren Sie im Block **Kompatibilität** das Kontrollkästchen **Ressourcen für andere Programme freigeben**.

FUNKTIONSPARAMETER FÜR KASPERSKY INTERNET SECURITY EXPORTIEREN / IMPORTIEREN

Kaspersky Internet Security bietet Ihnen die Möglichkeit, seine Programmeinstellungen zu exportieren und zu importieren.

Diese Option kann beispielsweise von Nutzen sein, wenn Sie Kaspersky Internet Security auf Ihrem PC zuhause und im Büro installiert haben. Sie können das Programm zu Hause entsprechend konfigurieren, die Einstellungen auf einer Diskette speichern und mit Hilfe der Importfunktion schnell auf Ihren Computer im Büro laden. Die Einstellungen werden in einer speziellen Konfigurationsdatei gespeichert.

- *Gehen Sie folgendermaßen vor, um die aktuellen Funktionsparameter von Kaspersky Internet Security zu exportieren:*

  1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.

  2. Wählen Sie im folgenden Fenster den Abschnitt **Einstellungen**.

  3. Klicken Sie im Block **Programmkonfiguration verwalten** auf die Schaltfläche **Speichern**.

  4. Geben Sie im folgenden Fenster einen Namen für die Konfigurationsdatei an und wählen Sie einen Speicherort dafür aus.

- *Gehen Sie folgendermaßen vor, um die Funktionsparameter aus einer Konfigurationsdatei zu importieren:*

  1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.

2. Wählen Sie im folgenden Fenster den Abschnitt **Einstellungen**.

3. Klicken Sie im Block **Programmkonfiguration verwalten** auf die Schaltfläche **Laden**.

4. Wählen Sie im folgenden Fenster eine Datei aus, aus der Sie die Parameter für Kaspersky Internet Security importieren möchten.

STANDARDPARAMETER WIEDERHERSTELLEN

Sie können jederzeit zu den empfohlenen Einstellungen für Kaspersky Internet Security zurückkehren. Diese gelten als optimal und werden von Kaspersky Lab empfohlen. Die Einstellungen werden durch den Schnellstartassistenten (s. Abschnitt "Schnellstartassistent" auf S. 30) des Programms wiederhergestellt.

Im folgenden Fenster können Sie angeben, welche Parameter bei der Wiederherstellung der empfohlenen Sicherheitsstufe beibehalten werden sollen und für welche Komponenten diese gelten sollen.

Die Liste enthält die Komponenten von Kaspersky Internet Security, deren Parameter vom Benutzer verändert oder von Kaspersky Internet Security beim Training der Komponenten Firewall und Anti-Spam gesammelt wurden. Wenn für eine bestimmte Komponente bei der Arbeit unikale Parameter festgelegt wurden, werden diese ebenfalls in der Liste angegeben.

Als unikale Parameter gelten: weiße und schwarze Listen mit Phrasen und Adressen für die Komponente Anti-Spam, Listen mit vertrauenswürdigen Internetadressen und Telefonnummern von Internetprovidern, die von den Komponenten Web-Anti-Virus und Anti-Spy verwendet werden, für den Schutz geltende Ausnahmeregeln, Filterregeln für Pakete und Programme für die Komponente Firewall.

Diese Listen werden während der Arbeit von Kaspersky Internet Security erstellt. Dabei werden individuelle Aufgaben und Sicherheitsanforderungen berücksichtigt. Das Erstellen der Listen ist sehr zeitaufwändig. Deshalb wird empfohlen, sie beim Wiederherstellen der ursprünglichen Programmeinstellungen zu speichern.

Nach dem Abschluss des Assistenten wird für alle Schutzkomponenten die Sicherheitsstufe **Empfohlen** eingestellt, wobei die von Ihnen zum Speichern gewählten Parameter berücksichtigt werden. Zusätzlich werden die Einstellungen übernommen, die Sie während der Arbeit des Assistenten vorgenommen haben.

➧ *Gehen Sie folgendermaßen vor, um die Schutzeinstellungen wiederherzustellen:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.

2. Wählen Sie im folgenden Fenster den Abschnitt **Einstellungen**.

3. Klicken Sie im Block **Programmkonfiguration verwalten** auf die Schaltfläche **Wiederherstellen**.

4. Aktivieren Sie im folgenden Fenster die Kontrollkästchen der Parameter, die gespeichert werden sollen. Klicken Sie auf **Weiter**. Dadurch wird der Konfigurationsassistent gestartet. Folgen Sie den Anweisungen.

BEDROHUNGEN UND AUSNAHMEN

Im Abschnitt **Bedrohungen und Ausnahmen** des Konfigurationsfensters von Kaspersky Internet Security können Sie:

- Kategorie der erkennbaren Bedrohungen auswählen (s. Abschnitt "Kategorien der erkennbaren Bedrohungen auswählen" auf S. 174);

- eine vertrauenswürdige Zone für das Programm anlegen.

Die *vertrauenswürdige Zone* ist eine benutzerdefinierte Liste von Objekten, die nicht von dem Programm kontrolliert werden. Mit anderen Worten ist dies eine Auswahl von Ausnahmen für den Schutz, den Kaspersky Internet Security bietet.

Die Vertrauenswürdige Zone wird mit der Liste vertrauenswürdigen Programme (s. Abschnitt "Vertrauenswürdige Programme auswählen" auf S. 174) und mit Ausnahmeregeln (s. Abschnitt "Ausnahmeregeln" auf S. 175) gebildet.

Die vertrauenswürdige Zone wird vom Benutzer unter Berücksichtigung der Besonderheiten von Objekten, mit denen er arbeitet, sowie von Programmen, die auf seinem Computer installiert sind, aufgebaut. Das Anlegen einer solchen Liste mit Ausnahmen kann beispielsweise erforderlich sein, wenn das Programm den Zugriff auf ein bestimmtes Objekt oder Programm blockiert, Sie aber sicher sind, dass dieses Objekt / Programm absolut unschädlich ist.

SIEHE AUCH

Kategorien der erkennbaren Bedrohungen auswählen 174

Vertrauenswürdige Programme auswählen 174

Regeln für Ausnahmen 175

Zulässige Ausschlussmasken für Dateien 176

Zulässige Masken für Bedrohungen 177

KATEGORIEN DER ERKENNBAREN BEDROHUNGEN AUSWÄHLEN

Kaspersky Internet Security bietet Ihnen Schutz vor verschiedenen Arten schädlicher Programme. Unabhängig von den festgelegten Parametern untersucht und neutralisiert das Programm immer Viren, trojanische Programme und Hackerprogramme. Diese Programme können Ihrem Computer bedeutenden Schaden zufügen. Um die Sicherheit des Computers zu erhöhen, können Sie die Liste der erkennbaren Bedrohungen erweitern. Aktivieren Sie dazu die Kontrolle für unterschiedliche Arten potentiell gefährlicher Programme.

Gehen Sie folgendermaßen vor, um die Kategorien erkennbare Bedrohungen auszuwählen:

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.

2. Wählen Sie im folgenden Fenster den Abschnitt **Gefahren und Ausnahmen** aus. Klicken Sie im Block **Bedrohungen** auf die Schaltfläche **Einstellungen**.

3. Wählen Sie im folgenden Fenster **Bedrohungen** die Bedrohungskategorien, vor denen Sie Ihren Computer schützen möchten.

VERTRAUENSWÜRDIGE PROGRAMME AUSWÄHLEN

Sie können eine Liste mit vertrauenswürdigen Programmen erstellen, deren Datei- und Netzwerkaktivität (einschließlich verdächtiger Aktivität) sowie deren Zugriffe auf die Systemregistrierung nicht kontrolliert werden sollen.

Sie halten beispielsweise die Objekte, die von dem standardmäßigen Microsoft Windows-Programm „Editor“ verwendet werden, für ungefährlich und deren Untersuchung im Schutz nicht für erforderlich. Das bedeutet, dass Sie diesem Programm vertrauen. Um die Objekte, die von diesem Prozess benutzt werden, von der Untersuchung auszuschließen, fügen Sie das Programm Editor zur Liste der vertrauenswürdigen Programme hinzu. Zugleich werden die ausführbare Datei und der Prozess eines vertrauenswürdigen Programms weiterhin auf Viren untersucht. Um ein Programm vollständig von der Untersuchung auszuschließen, müssen die Ausnahmeregeln verwendet werden.

Einige Aktionen, die als gefährlich klassifiziert werden, sind im Rahmen der Funktionalität bestimmter Programme normal. Beispielsweise ist das Abfangen eines Texts, den Sie über die Tastatur eingeben, für Programme zum automatischen Umschalten der Tastaturbelegung (Punto Switcher u.ä.) eine normale Aktion. Um die Besonderheit solcher Programme zu berücksichtigen und die Kontrolle ihrer Aktivität abzuschalten, empfehlen wir, sie in die Liste der vertrauenswürdigen Anwendungen aufzunehmen.

Durch das Ausschließen vertrauenswürdiger Programme aus der Untersuchung wird es erlaubt, Kompatibilitätsprobleme von Kaspersky Internet Security mit anderen Programmen zu lösen (beispielsweise das Problem einer doppelten Untersuchung des Netzwerkverkehrs eines anderen Computers durch Kaspersky Internet Security und durch ein anderes Antiviren-Programm). Außerdem lässt sich auf diese Weise die Leistungsfähigkeit des Computers erhöhen, was insbesondere bei der Verwendung von Serveranwendungen wichtig ist.

Kaspersky Internet Security untersucht standardmäßig alle Objekte, die von einem beliebigen Programmprozess geöffnet, gestartet oder gespeichert werden sollen, und kontrolliert die Aktivität aller Programme und den von ihnen erzeugten Netzwerkverkehr.

Gehen Sie folgendermaßen vor, um ein Programm zur Liste der vertrauenswürdigen Programme hinzuzufügen:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie im folgenden Fenster den Abschnitt **Gefahren und Ausnahmen** aus.
3. Klicken Sie im Block **Ausnahmen** auf die Schaltfläche **Einstellungen**.
4. Klicken Sie im folgenden Fenster auf der Registerkarte **Vertrauenswürdige Programme** auf den Link **Hinzufügen**.
5. Wählen Sie im Kontextmenü ein Programm aus. Bei Auswahl des Punkts **Durchsuchen** wird ein Fenster geöffnet, in dem der Pfad der ausführbaren Datei angegeben werden muss. Bei Auswahl des Punkts **Programme** wird eine Liste der momentan aktiven Programme geöffnet.
6. Legen Sie im folgenden Fenster **Ausnahmen für Programme** die Parameter der Ausnahmeregel fest.

Beachten Sie, dass nur der Datenverkehr des angegebenen Programms nicht auf Viren und Spam untersucht wird, wenn das Kontrollkästchen **Netzwerkverkehr nicht untersuchen** aktiviert wurde. Allerdings hat dies keinen Einfluss auf die Untersuchung des Datenverkehrs durch die Komponente Firewall, nach deren Parametern die Netzwerkaktivität des Programms analysiert wird.

Mit Hilfe der entsprechenden Links im unteren Bereich der Registerkarte können Sie ein vertrauenswürdiges Programm aus der Liste ändern oder löschen. Um ein Programm aus der Liste auszuschließen, ohne sie zu entfernen, deaktivieren Sie das Kontrollkästchen neben dem Programm.

REGELN FÜR AUSNAHMEN

Ein potentiell gefährliches Programm besitzt keine schädlichen Funktionen, kann aber von einem Schadprogramm als Hilfskomponente benutzt werden, weil es Schwachstellen und Fehler enthält. Zu dieser Kategorie gehören beispielsweise Programme zur Remote-Verwaltung, IRC-Clients, FTP-Server, alle Hilfsprogramme zum Beenden von Prozessen und zum Verstecken ihrer Arbeit, Tastaturspione, Programme zur Kennwortermittlung, Programme zur automatischen Einwahl auf kostenpflichtige Seiten usw. Solche Software wird nicht als Virus klassifiziert (not-a-virus). Sie lässt sich beispielsweise in folgende Typen unterteilen: Adware, Joke, Riskware u.a. (ausführliche Informationen über potentiell gefährliche Programme, die von Kaspersky Internet Security erkannt werden, finden Sie in der Viren-Enzyklopädie auf der Seite www.viruslist.com/de). Derartige Programme können aufgrund der Untersuchung gesperrt werden. Da bestimmte Programme dieser Kategorie von vielen Benutzern verwendet werden, besteht die Möglichkeit, sie von der Untersuchung auszuschließen.

Es kann beispielsweise sein, dass Sie häufig mit dem Programm Remote Administrator arbeiten. Dabei handelt es sich um ein Programm, das dem Remote-Zugriff dient und die Arbeit auf einem Remote-Computer erlaubt. Diese Anwendungsaktivität wird von Kaspersky Internet Security als potentiell gefährlich eingestuft und kann blockiert werden. Um zu verhindern, dass das Programm gesperrt wird, muss eine Ausnahmeregel für das Programm erstellt werden, die sie entsprechend der Viren-Enzyklopädie als *not-a-virus:RemoteAdmin.Win32.RAdmin.22* erkennt.

Eine *Ausnahmeregel* ist eine Kombination von Bedingungen, bei deren Vorhandensein ein Objekt nicht von Kaspersky Internet Security untersucht wird.

Von der Untersuchung können Dateien eines bestimmten Formats, Dateien nach Maske, bestimmte Bereiche (beispielsweise ein Ordner oder Programm) sowie Programmprozesse oder Objekte nach einem Bedrohungstyp gemäß der Klassifikation der Viren-Enzyklopädie ausgeschlossen werden.

Ein *Bedrohungstyp* ist ein Status, der einem Objekt bei der Untersuchung von Kaspersky Internet Security zugewiesen wird. Der Bedrohungstyp beruht auf der Klassifikation schädlicher und potentiell gefährlicher Programme, die in der Viren-Enzyklopädie von Kaspersky Lab enthalten ist.

Beim Hinzufügen einer Ausnahme wird eine Regel erstellt, die danach einige Programmkomponenten verwenden können (Beispiel Datei-Anti-Virus (s. Abschnitt "Schutz für das Dateisystem des Computers" auf S. 47), Mail-Anti-Virus (s. Abschnitt "E-Mail-Schutz" auf S. 57), Web-Anti-Virus (s. Abschnitt "Schutz für Web-Datenverkehr" auf S. 64)) und ebenso die Aufgaben der Virenuntersuchung.

Gehen Sie folgendermaßen vor, um eine Ausnahmeregel zu erstellen:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie im folgenden Fenster den Abschnitt **Gefahren und Ausnahmen** aus.
3. Klicken Sie im Block **Ausnahmen** auf die Schaltfläche **Einstellungen**.
4. Klicken Sie im folgenden Fenster auf der Registerkarte **Regeln für Ausnahmen** auf den Link **Hinzufügen**.
5. Geben Sie im folgenden Fenster **Ausnahmeregel** die Parameter der Ausnahmeregel an.

SIEHE AUCH

Zulässige Ausschlussmasken für Dateien 176

Zulässige Masken für Bedrohungen 177

ZULÄSSIGE AUSSCHLUSSMASKEN FÜR DATEIEN

Hier werden Beispiele für zulässige Masken genannt, die Sie beim Erstellen der Liste auszuschließender Dateien verwenden können. Dazu gehören:

1. Masken ohne Dateipfad:
   - ***.exe** – alle Dateien mit der Endung *exe*;
   - ***.ex?** – alle Dateien mit der Endung *ex?*, wobei anstelle von **?** ein beliebiges Zeichen stehen kann.
   - **test** – alle Dateien mit dem Namen *test*
2. Masken mit absolutem Dateipfad:
   - **C:\dir*.*** oder **C:\dir*** oder **C:\dir** - alle Dateien im Ordner *C:\dir*;
   - **C:\dir*.exe** – alle Dateien mit der Endung *exe* im Ordner C:\dir\;
   - **C:\dir*.ex?** – alle Dateien mit der Endung *ex?* im Ordner *C:\dir*, wobei anstelle von **?** ein beliebiges Zeichen stehen kann;
   - **C:\dir\test** – nur die Datei *C:\dir\test*.

     Um zu verhindern, dass die Dateien in allen untergeordneten Ordnern des gewählten Ordners untersucht werden, aktivieren Sie beim Erstellen der Maske das Kontrollkästchen **Unterordner einschließen**.
3. Masken mit Dateipfad:
   - **dir*.*** oder **dir*** oder **dir** - alle Dateien in allen Ordnern von *dir*;
   - **dir\test** – alle Dateien mit dem Namen *test* in den Ordnern von *dir*;
   - **dir*.exe** – alle Dateien mit der Endung *exe* in allen Ordnern *dir*;

- **dir*.ex?** – alle Dateien mit der Endung *ex?* in allen Ordnern von *dir*\, wobei anstelle von **?** ein beliebiges Zeichen stehen kann.

  Um zu verhindern, dass die Dateien in allen untergeordneten Ordnern des gewählten Ordners untersucht werden, aktivieren Sie beim Erstellen der Maske das Kontrollkästchen **Unterordner einschließen**.

Die Verwendung der Ausnahmemaske *.* oder * ist nur zulässig, wenn die auszuschließende Bedrohung gemäß der Viren-Enzyklopädie klassifiziert wird. In diesem Fall wird die Bedrohung nicht in allen Objekten gefunden werden. Wenn diese Masken ohne Angabe einer Klassifikation verwendet werden, entspricht dies dem Deaktivieren des Schutzes. Außerdem wird davor gewarnt, den Pfad eines virtuellen Laufwerks, das auf Basis eines Dateisystemordners mit dem Befehl subst erstellt wurde, oder den Pfad eines Laufwerks, das der Mirror eines Netzwerkordners ist, als Ausnahme auszuwählen. Es kann sein, dass für unterschiedliche Benutzer eines Computers ein identischer Laufwerksname unterschiedliche Ressourcen bezeichnet, was beim Auslösen von Ausnahmeregeln unvermeidlich zu Fehlern führt.

ZULÄSSIGE MASKEN FÜR BEDROHUNGEN

Wenn eine Bedrohung, die ein bestimmtes Verdikt nach der Klassifikation der Viren-Enzyklopädie besitzt, als Ausnahme hinzugefügt wird, können Sie angeben:

- den vollständigen Namen der Bedrohung, wie er in der Viren-Enzyklopädie auf der Seite *www.viruslist.com/de* genannt wird (beispielsweise *not-a-virus:RiskWare.RemoteAdmin.RA.311* oder *Flooder.Win32.Fuxx*).
- den Namen der Bedrohung als Maske, beispielsweise:
  - **not-a-virus*** – Legale, aber potentiell gefährliche Programme sowie Scherzprogramme von der Untersuchung ausschließen.
  - ***Riskware.*** – Alle potentiell gefährlichen Programme des Typs Riskware von der Untersuchung ausschließen.
  - ***RemoteAdmin.*** – Alle Versionen von Programmen zur Fernverwaltung von der Untersuchung ausschließen.

NETZWERK

Im Abschnitt **Netzwerk** des Programmkonfigurationsfensters können Sie die Ports, die von Kaspersky Internet Security kontrolliert werden sollen, auswählen und die Untersuchung geschützter Verbindungen anpassen:

- Liste der zu kontrollierenden Ports erstellen (s. S. 178);
- Modus zur Untersuchung geschützter Verbindungen (mit dem Protokoll SSL) aktivieren / deaktivieren (s. S. 179).
- Proxyserver-Parameter anpassen (s. S. 181).
- Zugriff auf die Analyse von Netzwerkpaketen öffnen (s. S. 181).

SIEHE AUCH

Liste der zu kontrollierenden Ports erstellen 178

Untersuchung geschützter Verbindungen 179

Untersuchung geschützter Verbindungen in Mozilla Firefox 179

Untersuchung geschützter Verbindungen in Opera 180

Proxyserver-Einstellungen 181

Zugriff auf die Analyse von Netzwerkpaketen 181

LISTE DER ZU KONTROLLIERENDEN PORTS ERSTELLEN

Solche Schutzkomponenten wie Mail-Anti-Virus (s. Abschnitt "E-Mail-Schutz" auf S. 57), Web-Anti-Virus (s. Abschnitt "Schutz für Web-Datenverkehr" auf S. 64) und Anti-Spam (auf S. 103) kontrollieren die Datenströme, die durch bestimmte Protokolle übertragen werden und über bestimmte geöffnete Ports in Ihren Computer eintreffen. Mail-Anti-Virus analysiert beispielsweise die Informationen, die mit dem Protokoll SMTP übertragen werden, Web-Anti-Virus analysiert HTTP-Pakete.

Für die Kontrolle der Ports stehen zwei Modi zur Auswahl:

- **Alle Netzwerkports kontrollieren**.
- **Nur ausgewählte Ports kontrollieren**. Eine Liste der Ports, die gewöhnlich zur Übertragung von E-Mails und HTTP-Datenstrom benutzt werden, gehört zum Lieferumfang des Programms.

Gehen Sie folgendermaßen vor, um einen Port zur Liste der kontrollierten Ports hinzuzufügen:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie im folgenden Fenster den Abschnitt **Netzwerk**.
3. Klicken Sie im Block **Kontrollierte Ports** auf die Schaltfläche **Auswählen**.
4. Klicken Sie im folgenden Fenster **Netzwerkports** auf den Link **Hinzufügen**.
5. Geben Sie im folgenden Fenster **Netzwerkport** die notwendigen Daten an.

Gehen Sie folgendermaßen vor, um einen Port aus der Liste der kontrollierten Ports auszuschließen:

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
2. Wählen Sie im folgenden Fenster den Abschnitt **Netzwerk**.
3. Klicken Sie im Block **Kontrollierte Ports** auf die Schaltfläche **Auswählen**.
4. Deaktivieren Sie im folgenden Fenster **Netzwerkports** das Kontrollkästchen neben der Beschreibung des Ports.

Gehen Sie folgendermaßen vor, um eine Liste der Programme anzulegen, für die alle Ports kontrolliert werden sollen:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.

2. Wählen Sie im folgenden Fenster den Abschnitt **Netzwerk**.

3. Klicken Sie im Block **Kontrollierte Ports** auf die Schaltfläche **Auswählen**.

4. Aktivieren Sie im folgenden Fenster **Netzwerkports** das Kontrollkästchen **Alle Ports für die angegebenen Programme kontrollieren** und klicken Sie im Block unten auf den Link **Hinzufügen**.

5. Wählen Sie im Kontextmenü ein Programm aus. Bei Auswahl des Punkts **Durchsuchen** wird ein Fenster geöffnet, in dem der Pfad der ausführbaren Datei angegeben werden muss. Bei Auswahl des Punkts **Programme** wird eine Liste der momentan aktiven Programme geöffnet.

6. Geben Sie im folgenden Fenster **Programm** eine Beschreibung für das ausgewählte Programm an.

UNTERSUCHUNG GESCHÜTZTER VERBINDUNGEN

Eine Verbindung unter Verwendung des SSL-Protokolls schützt den Datenaustausch. Das SSL-Protokoll erlaubt die Identifikation der am Datenaustausch beteiligten Partner. Dazu dienen elektronische Zertifikate. Außerdem werden die übertragenen Daten verschlüsselt und beim Übertragungsvorgang wird die Datenintegrität gewährleistet.

Diese Besonderheiten des Protokolls werden aber von Angreifern zur Verbreitung schädlicher Programme benutzt, weil die meisten Antiviren-Produkte den SSL-Verkehr nicht untersuchen.

Die Untersuchung von geschützten Verbindungen wird in Kaspersky Internet Security realisiert, indem ein Zertifikat von Kaspersky Lab installiert wird. Dieses Zertifikat wird immer verwendet, um die Sicherheit einer Verbindung zu prüfen.

Die Untersuchung des Datenverkehrs nach dem SSL-Protokoll findet künftig mit Hilfe des installierten Kaspersky-Lab-Zertifikats statt. Wenn bei der Verbindung mit einem Server ein inkorrektes Zertifikat gefunden wird (wenn es z.B. von einem ein Angreifer ausgetauscht wurde), erscheint auf dem Bildschirm eine Meldung, in der Sie das Zertifikat akzeptieren oder ablehnen, oder Informationen über das Zertifikat anzeigen können. Wenn das Programm im automatischen Modus arbeitet, werden Verbindungen, die ein inkorrektes Zertifikat verwenden, ohne Nachfrage getrennt.

➡ *Gehen Sie folgendermaßen vor, um die Untersuchung geschützter Verbindungen zu aktivieren:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.

2. Wählen Sie im folgenden Fenster den Abschnitt **Netzwerk**.

3. Aktivieren Sie im folgenden Fenster das Kontrollkästchen **Geschützte Verbindungen untersuchen** und klicken Sie auf die Schaltfläche **Zertifikat installieren**.

4. Klicken Sie im folgenden Fenster auf die Schaltfläche **Zertifikat installieren**. Es wird ein Assistent gestartet, der Sie bei der Installation eines Zertifikats unterstützt.

Die automatische Installation eines Zertifikats erfolgt nur bei der Arbeit mit dem Browser Microsoft Internet Explorer. Zur Untersuchung von geschützten Verbindungen in den Browsern Mozilla Firefox und Opera muss das Kaspersky-Lab-Zertifikat manuell installiert werden.

UNTERSUCHUNG GESCHÜTZTER VERBINDUNGEN IN MOZILLA FIREFOX

Der Browser Mozilla Firefox verwendet nicht den Zertifikatsspeicher von Microsoft Windows. Bei der Verwendung von Firefox ist es zur Untersuchung von SSL-Verbindungen erforderlich, das Kaspersky-Lab-Zertifikat manuell zu installieren.

➡ *Gehen Sie folgendermaßen vor, um das Kaspersky-Lab-Zertifikat zu installieren:*

1. Wählen Sie im Menü des Browsers den Punkt **Tools** → **Einstellungen**.

2. Wählen Sie im folgenden Fenster den Abschnitt **Erweitert**.

3. Wählen Sie im Block **Zertifikate** die Registerkarte **Sicherheit** und klicken Sie auf die Schaltfläche **Zertifikate anzeigen**.

4. Wählen Sie im folgenden Fenster die Registerkarte **Zertifizierungsstellen** und klicken Sie auf die Schaltfläche **Importieren**.

5. Wählen Sie im folgenden Fenster die Datei des Kaspersky-Lab-Zertifikats. Pfad der Datei des Kaspersky-Lab-Zertifikats: *%AllUsersProfile%\Application Data\Kaspersky Lab\AVP8\Data\Cert\(fake)Kaspersky Anti-Virus personal root certificate.cer*.

6. Aktivieren Sie im folgenden Fenster die Kontrollkästchen der Aktionen, für deren Untersuchung das installierte Zertifikat verwendet werden soll. Anzeige von Informationen zu dem Zertifikat dient die Schaltfläche **Ansicht**.

Gehen Sie folgendermaßen vor, um das Kaspersky-Lab-Zertifikat für Mozilla Firefox Version 3.x zu installieren:

1. Wählen Sie im Menü des Browsers den Punkt **Tools** → **Konfiguration**.

2. Wählen Sie im folgenden Fenster den Abschnitt **Erweitert**.

3. Klicken Sie auf der Registerkarte **Verschlüsselung** auf die Schaltfläche **Zertifikate anzeigen**.

4. Wählen Sie im folgenden Fenster die Registerkarte **Zertifizierungsstellen** und klicken Sie auf die Schaltfläche **Importieren**.

5. Wählen Sie im folgenden Fenster die Datei des Kaspersky-Lab-Zertifikats. Pfad der Datei des Kaspersky-Lab-Zertifikats: *%AllUsersProfile%\Application Data\Kaspersky Lab\AVP8\Data\Cert\(fake)Kaspersky Anti-Virus personal root certificate.cer*.

6. Aktivieren Sie im folgenden Fenster die Kontrollkästchen der Aktionen, für deren Untersuchung das installierte Zertifikat verwendet werden soll. Anzeige von Informationen zu dem Zertifikat dient die Schaltfläche **Anzeigen**.

Wenn Ihr Computer mit dem Betriebssystem Microsoft Windows Vista arbeitet, lautet der Pfad der Zertifikatsdatei von Kaspersky Lab: *%AllUsersProfile%\Kaspersky Lab\AVP8\Data\Cert\(fake)Kaspersky Anti-Virus personal root certificate.cer*.

UNTERSUCHUNG GESCHÜTZTER VERBINDUNGEN IN OPERA

Der Browser Opera verwendet nicht den Zertifikatsspeicher von Microsoft Windows. Bei der Verwendung von Opera ist es zur Untersuchung von SSL-Verbindungen erforderlich, das Kaspersky-Lab-Zertifikat manuell zu installieren.

Gehen Sie folgendermaßen vor, um das Kaspersky-Lab-Zertifikat zu installieren:

1. Wählen Sie im Menü des Browsers den Punkt **Tools** → **Konfiguration**.

2. Wählen Sie im folgenden Fenster den Abschnitt **Erweitert**.

3. Wählen Sie auf der linken Fensterseite die Registerkarte **Sicherheit** und klicken Sie auf die Schaltfläche **Zertifikate verwalten**.

4. Wählen Sie im folgenden Fenster die Registerkarte **Zertifizierungsstellen** und klicken Sie auf die Schaltfläche **Importieren**.

5. Wählen Sie im folgenden Fenster die Datei des Kaspersky-Lab-Zertifikats. Pfad der Datei des Kaspersky-Lab-Zertifikats: *%AllUsersProfile%\Application Data\Kaspersky Lab\AVP8\Data\Cert\(fake)Kaspersky Anti-Virus personal root certificate.cer*.

6. Klicken Sie im folgenden Fenster auf die Schaltfläche **Installieren**. Das Kaspersky-Lab-Zertifikat wird installiert. Um Informationen zum Zertifikat anzuzeigen und die Aktionen, bei denen das Zertifikat verwendet werden soll, auszuwählen, wählen Sie das Zertifikat in der Liste aus und klicken Sie auf die Schaltfläche **Anzeigen**.

Gehen Sie folgendermaßen vor, um das Kaspersky-Lab-Zertifikat für Opera Version 9.x zu installieren:

1. Wählen Sie im Menü des Browsers den Punkt **Tools** → **Einstellungen**.
2. Wählen Sie im folgenden Fenster den Abschnitt **Erweitert**.
3. Wählen Sie auf der linken Fensterseite die Registerkarte **Sicherheit** und klicken Sie auf die Schaltfläche **Zertifikate verwalten**.
4. Wählen Sie im folgenden Fenster die Registerkarte **Zertifizierungsstellen** und klicken Sie auf die Schaltfläche **Importieren**.
5. Wählen Sie im folgenden Fenster die Datei des Kaspersky-Lab-Zertifikats. Pfad der Datei des Kaspersky-Lab-Zertifikats: *%AllUsersProfile%\Application Data\Kaspersky Lab\AVP8\Data\Cert\(fake)Kaspersky Anti-Virus personal root certificate.cer*.
6. Klicken Sie im folgenden Fenster auf die Schaltfläche **Installieren**. Das Kaspersky-Lab-Zertifikat wird installiert.

Wenn Ihr Computer mit dem Betriebssystem Microsoft Windows Vista arbeitet, lautet der Pfad der Zertifikatsdatei von Kaspersky Lab: *%AllUsersProfile%\Kaspersky Lab\AVP8\Data\Cert\(fake)Kaspersky Anti-Virus personal root certificate.cer*.

PROXYSERVER-EINSTELLUNGEN

Wenn die Internetverbindung über einen Proxyserver erfolgt, ist es erforderlich, die entsprechenden Verbindungsparameter anzupassen. Kaspersky Internet Security verwendet diese Parameter bei der Arbeit bestimmter Schutzkomponenten und für das Update der Datenbanken und Programm-Module.

Wenn in Ihrem Netzwerk ein Proxyserver verwendet wird, der einen nicht standardmäßigen Port benutzt, ist es erforderlich, diesen Port zur Liste der kontrollierten Ports hinzuzufügen (s. Abschnitt "Liste der zu kontrollierenden Ports erstellen" auf S. 178).

Gehen Sie folgendermaßen vor, um die Proxyserver-Parameter anzupassen:

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
2. Wählen Sie im folgenden Fenster den Abschnitt **Netzwerk**.
3. Klicken Sie im Block **Proxyserver** auf die Schaltfläche **Proxyserver anpassen**.
4. Ändern Sie im folgenden Fenster **Proxyserver-Einstellungen** die Parameter für den Proxyserver.

ZUGRIFF AUF DIE ANALYSE VON NETZWERKPAKETEN

Das Werkzeug **Analyse von Netzwerkpaketen** ist für erfahrene Anwender gedacht, die sich mit der Struktur von Netzwerken und Netzwerkprotokollen auskennen.

Kaspersky Internet Security bietet das Werkzeug *Analyse von Netzwerkpaketen*. Dieses Werkzeug dient zum Sammeln und zur Analyse der Netzwerkaktivität im Netzwerk, zu dem Ihr Computer gehört.

Die Analyse von Netzwerkpaketen steht in der Grundeinstellung nicht im Hauptfenster von Kaspersky Internet Security zur Verfügung.

Gehen Sie folgendermaßen vor, um den Zugriff auf die Analyse von Netzwerkpaketen zu öffnen:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie im folgenden Fenster den Abschnitt **Netzwerk**.
3. Aktivieren Sie im Block **Analyse von Netzwerkpaketen** das Kontrollkästchen **Monitor "Analyse von Netzwerkpaketen" anzeigen**.

MELDUNGEN

Bei der Arbeit von Kaspersky Internet Security treten unterschiedliche Ereignisse ein. Sie können informativen Charakter besitzen oder wichtige Informationen enthalten. Ein Ereignis kann beispielsweise über die erfolgreiche Aktualisierung des Programms informieren oder einen Fehler bei der Arbeit einer bestimmten Komponente festhalten, der dringend behoben werden muss.

Um sich über die Ereignisse bei der Arbeit von Kaspersky Internet Security informieren zu lassen, verwenden Sie den Dienst für Benachrichtigungen.

In der Grundeinstellung dienen Popupmeldungen und entsprechende Tonsignale zur Benachrichtigung des Benutzers.

Die Meldungen können durch eine der folgenden Methoden erfolgen:

- Popupmeldungen über dem Programmsymbol im Infobereich der Taskleiste
- Tonsignale.
- E-Mail-Nachrichten.

Gehen Sie folgendermaßen vor, um das Senden von Meldungen zu deaktivieren:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie im folgenden Fenster den Abschnitt **Meldungen**.
3. Deaktivieren Sie das Kontrollkästchen **Über Ereignisse benachrichtigen**.

Auch wenn das Senden von Meldungen deaktiviert wurde, werden Informationen über Ereignisse, die bei der Arbeit von Kaspersky Internet Security eintreten, im Bericht über die Programmarbeit aufgezeichnet.

Gehen Sie folgendermaßen vor, um eine Methode für das Senden von Meldungen auszuwählen:

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
2. Wählen Sie im folgenden Fenster den Abschnitt **Meldungen** und klicken Sie auf die Schaltfläche **Einstellungen**.
3. Wählen Sie im folgenden Fenster **Meldungen** eine Methode für das Senden von Meldungen aus.

SIEHE AUCH

Audiosignale zur Begleitung von Benachrichtigungen deaktivieren 183

E-Mail-Benachrichtigungen senden 183

AUDIOSIGNALE ZUR BEGLEITUNG VON BENACHRICHTIGUNGEN DEAKTIVIEREN

In der Grundeinstellung werden alle Meldungen von einem Audiosignal begleitet. Dazu wird das Soundschema von Microsoft Windows verwendet. Das Kontrollkästchen **Standardsoundschema Windows Default verwenden** erlaubt es, das verwendete Schema zu ändern. Wenn das Kontrollkästchen deaktiviert ist, wird das Soundschema der vorhergehenden Programmversion verwendet.

Gehen Sie folgendermaßen vor, um die Audiosignale zur Begleitung von Benachrichtigungen zu deaktivieren:

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
2. Wählen Sie im folgenden Fenster den Abschnitt **Meldungen**.
3. Deaktivieren Sie das Kontrollkästchen **Audiosignale für Meldungen aktivieren**.

E-MAIL-BENACHRICHTIGUNGEN SENDEN

Für das Senden von E-Mail-Benachrichtigungen ist es erforderlich, die E-Mail-Parameter anzupassen.

Gehen Sie folgendermaßen vor, um die E-Mail-Parameter für das Senden von Meldungen anzupassen:

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
2. Wählen Sie im folgenden Fenster den Abschnitt **Meldungen**.
3. Aktivieren das Kontrollkästchen **E-Mails über Ereignisse senden** und klicken Sie auf die Schaltfläche **E-Mail-Einstellungen**.
4. Geben Sie im folgenden Fenster **E-Mail-Meldungen anpassen** die Versandparameter an.

BERICHTE UND SPEICHER

Dieser Abschnitt enthält Parameter, die die Arbeit mit der Datenverwaltung von Kaspersky Internet Security regulieren.

Die *Datenverwaltung der Anwendung* umfasst Objekte, die während der Arbeit von Kaspersky Internet Security in der Quarantäne und im Backup gespeichert wurden, sowie Berichte über die Arbeit der Programmkomponenten.

In diesem Abschnitt können Sie:

- Einstellungen für die Erstellung (s. S. 184) und Speicherung von Berichten (s. S. 184) konfigurieren;
- Einstellungen für Quarantäne und Backup (s. S. 186) konfigurieren.

SIEHE AUCH

Einträge über Ereignisse zum Bericht hinzufügen 184

Berichte leeren 184

Berichte speichern 184

Quarantäne für möglicherweise infizierte Objekte 185

Sicherungskopien gefährlicher Objekte 186

Arbeit mit Objekten in der Quarantäne 186

Quarantäne- und Backup-Objekte speichern 186

Berichte 199

EINTRÄGE ÜBER EREIGNISSE ZUM BERICHT HINZUFÜGEN

Sie können festlegen, dass dem Schutzbericht auch Einträge über unkritische Ereignisse sowie Ereignisse, die die Registrierung und das Dateisystem betreffen, hinzugefügt werden. In der Grundeinstellung werden diese Einträge nicht zum Bericht hinzugefügt.

- *Gehen Sie folgendermaßen vor, damit dem Schutzbericht auch Einträge über unkritische Ereignisse sowie über Ereignisse der Registrierung und / oder des Dateisystems hinzugefügt werden:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
2. Wählen Sie im folgenden Fenster den Abschnitt **Berichte und Speicher** aus.
3. Aktivieren Sie im Block **Berichte** das entsprechende Kontrollkästchen ☑.

BERICHTE LEEREN

Informationen über die Arbeit von Kaspersky Internet Security werden in den Berichten aufgezeichnet. Diese können bereinigt werden.

- *Um die* Berichte zu leeren, *machen Sie Folgendes*:

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
2. Wählen Sie im folgenden Fenster den Abschnitt **Berichte und Speicher**.
3. Klicken Sie im Block **Berichte** auf die Schaltfläche **Leeren**.
4. Aktivieren Sie im folgenden Fenster **Informationen aus Berichten löschen** die Kontrollkästchen der Berichtskategorien, die Sie bereinigen möchten.

BERICHTE SPEICHERN

Sie können die maximale Speicherdauer für Ereignisberichte festlegen (Kontrollkästchen ☑ **Berichte speichern für maximal**). Standardmäßig beträgt die Speicherdauer für Quarantäneobjekte 30 Tage. Danach werden die Objekte gelöscht. Die maximale Speicherdauer kann geändert oder völlig aufgehoben werden. Außerdem kann die Größe einer Berichtsdatei beschränkt werden (Kontrollkästchen ☑ **Maximale Dateigröße**). Die maximale Größe beträgt

standardmäßig 1024 MB. Wenn die maximale Größe erreicht wird, wird der Inhalt der Datei mit neuen Einträgen überschrieben. Sie können die Größenbeschränkung aufheben oder einen anderen Wert festlegen.

➡ *Gehen Sie folgendermaßen vor, um die Parameter für das Speichern von Berichten anzupassen:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.

2. Wählen Sie im folgenden Fenster den Abschnitt **Berichte und Speicher** aus.

3. Aktivieren Sie im folgenden Fenster im Block **Berichte** die entsprechenden Kontrollkästchen ☑ und ändern Sie, falls erforderlich, die maximale Berichtsgröße und die Speicherdauer.

QUARANTÄNE FÜR MÖGLICHERWEISE INFIZIERTE OBJEKTE

Die *Quarantäne* ist ein spezieller Speicher, in den Objekte verschoben werden, die möglicherweise von Viren infiziert sind.

Möglicherweise infizierte Objekte sind Objekte, die verdächtig werden, von Viren oder Virenmodifikationen infiziert zu sein.

Ein verdächtiges Objekt kann während der Virensuche sowie bei der Arbeit von Datei-Anti-Virus, Mail-Anti-Virus und Proaktiver Schutz gefunden und in die Quarantäne verschoben werden.

Objekte werden aufgrund der Arbeit von Datei-Anti-Virus und Mail-Anti-Virus sowie während der Virensuche in die Quarantäne verschoben, wenn:

- *Der Code des analysierten Objekts besitzt Ähnlichkeit mit einer bekannten Bedrohung, wurde aber teilweise verändert*.

  Die Datenbanken von Kaspersky Internet Security enthalten jene Bedrohungen, die bisher von den Kaspersky-Lab-Spezialisten untersucht wurden. Wenn ein Schadprogramm verändert wird und diese Veränderungen noch nicht in die Signaturen aufgenommen wurden, klassifiziert Kaspersky Internet Security das Objekt, das von einem veränderten Schadprogramm infiziert ist, als möglicherweise infiziertes Objekt und informiert darüber, welcher Bedrohung diese Infektion ähnelt.

- *Der Code des gefundenen Objekts erinnert an die Struktur eines Schadprogramms. Die Bedrohungssignaturen enthalten jedoch keine entsprechenden Einträge*.

  Es ist durchaus möglich, dass es sich um eine neue Art von Bedrohung handelt. Deshalb klassifiziert Kaspersky Internet Security dieses Objekt als möglicherweise infiziertes Objekt.

Der Verdacht, dass eine Datei durch einen Virus infiziert ist, wird mit dem *heuristischen Code Analysator* ermittelt, mit dessen Hilfe bis zu 92 % neuer Viren erkannt werden. Dieser Mechanismus ist sehr effektiv und führt nur selten zu einem Fehlalarm.

Was den Proaktiven Schutz betrifft, so wird ein Objekt von der Komponente in die Quarantäne verschoben, wenn aufgrund der Analyse seines Verhaltens die Reihenfolge der Aktionen, die das Objekt ausführt, als verdächtig eingestuft wird.

Ein Objekt unter Quarantäne zu stellen, bedeutet, es wird nicht kopiert, sondern verschoben: Das Objekt wird am ursprünglichen Speicherort oder aus einer E-Mail-Nachricht gelöscht und im Quarantäneordner gespeichert. Die unter Quarantäne stehenden Dateien werden in einem speziellen Format gespeichert und stellen keine Gefahr dar.

Möglicherweise kann die Bedrohung von Kaspersky Internet Security eindeutig bestimmt und desinfiziert werden, nachdem die Datenbanken des Programms aktualisiert wurden. Deshalb untersucht das Programm die Quarantäneobjekte nach jedem Update (s. S. 154).

SICHERUNGSKOPIEN GEFÄHRLICHER OBJEKTE

Bei der Desinfektion von Objekten kann es vorkommen, dass es nicht gelingt, die Objekte vollständig zu erhalten. Wenn ein desinfiziertes Objekt wichtige Informationen enthielt, die aufgrund der Desinfektion vollständig oder teilweise verloren gingen, kann versucht werden, das ursprüngliche Objekt über seine Sicherungskopie wiederherzustellen.

Eine *Sicherungskopie* ist eine Kopie des gefährlichen Originalobjekts. Sie wird bei der ersten Desinfektion oder beim Löschen des Objekts erstellt und im Backup gespeichert.

Das *Backup* ist ein spezieller Speicher für Sicherungskopien gefährlicher Objekte, die verarbeitet oder gelöscht werden. Die wichtigste Funktion des Backups besteht in der Möglichkeit, das ursprüngliche Objekt jederzeit wiederherzustellen. Die Sicherungskopien werden im Backup in einem speziellen Format gespeichert und stellen keine Gefahr dar.

ARBEIT MIT OBJEKTEN IN DER QUARANTÄNE

Mit Objekten, die in die Quarantäne verschoben wurden, können Sie folgende Aktionen ausführen:

- Dateien, die Sie für infiziert halten, in die Quarantäne verschieben.
- Alle möglicherweise infizierten Quarantäneobjekte unter Verwendung der aktuellen Version der Datenbanken von Kaspersky Internet Security untersuchen und desinfizieren.
- Dateien wiederherstellen entweder in einem vom Benutzer gewählten Ordner oder in den Ordnern, aus denen sie (standardmäßig) in die Quarantäne verschoben wurden.
- Ein beliebiges Quarantäneobjekt oder eine Gruppe ausgewählter Objekte löschen.
- Quarantäneobjekte zur Untersuchung an Kaspersky Lab schicken.

Gehen Sie folgendermaßen vor, um mit Quarantäneobjekten zu arbeiten:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Quarantäne**.
2. Führen Sie im folgenden Fenster auf der Registerkarte **Erkannte Bedrohungen** die entsprechenden Aktionen aus.

QUARANTÄNE- UND BACKUP-OBJEKTE SPEICHERN

Sie können folgende Parameter für Quarantäne und Backup anpassen:

- Legen Sie eine maximale Speicherdauer für Objekte in der Quarantäne und Sicherungskopien im Backup fest (Kontrollkästchen ☑ **Objekte speichern für maximal**). Standardmäßig beträgt die Speicherdauer für Quarantäneobjekte 30 Tage. Danach werden die Objekte gelöscht. Sie können die maximale Speicherdauer ändern oder diese Beschränkung völlig aufheben.
- Eine maximale Größe für den Datenspeicher festlegen (Kontrollkästchen ☑ **Maximale Größe**). Die maximale Größe beträgt standardmäßig 100 MB. Sie können die Größenbeschränkung aufheben oder einen anderen Wert festlegen.

Gehen Sie folgendermaßen vor, um die Parameter für die Quarantäne und das Backup anzupassen:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie im folgenden Fenster den Abschnitt **Berichte und Speicher** aus.
3. Aktivieren Sie im Block **Quarantäne und Backup** die entsprechenden Kontrollkästchen und legen Sie bei Bedarf eine maximale Größe für den Datenspeicher fest.

FEEDBACK

Jeden Tag taucht eine Vielzahl neuer Bedrohungen auf. Um das Sammeln statistischer Daten über die Typen und Quellen neuer Bedrohungen zu beschleunigen und die Entwicklung entsprechender Neutralisierungsmethoden zu optimieren, bietet Kaspersky Lab Ihnen die Teilnahme an dem Dienst *Kaspersky Security Network* an.

Die Verwendung von Kaspersky Security Network sieht vor, dass bestimmte Informationen an Kaspersky Lab gesendet werden. Es werden folgende Daten gesendet:

- Individuelle ID, die Ihrem Computer vom Kaspersky Lab-Produkt zugewiesen wird. Dieser Identifikator charakterisiert die Hardwareparameter Ihres Computers und enthält keinerlei persönliche Informationen.
- Informationen über die Bedrohungen, die von den Programmkomponenten gefunden wurden. Die Auswahl der Informationen ist vom Typ der gefundenen Bedrohung abhängig.
- Informationen über das System: Version des Betriebssystems, installierte Service Packs, geladene Dienste und Treiber, Versionen von Browsern und Mailprogrammen, Erweiterungen für Browser, Versionsnummer des installierten Kaspersky-Lab-Programms.

Gehen Sie folgendermaßen vor, um das Senden einer Statistik an Kaspersky Security Network zu aktivieren:

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
2. Wählen Sie im folgenden Fenster den Abschnitt **Feedback** aus.
3. Aktivieren Sie das Kontrollkästchen **Ich akzeptiere die Teilnahmebedingungen für Kaspersky Security Network**.

AUSSEHEN DES PROGRAMMS

Sie können das Aussehen von Kaspersky Internet Security verändern, indem Sie unterschiedliche grafische Elemente und Farbschemen erstellen und verwenden. Zusätzlich besteht die Möglichkeit, aktive Elemente der Benutzeroberfläche anzupassen (Programmsymbol im Infobereich der Microsoft Windows-Taskleiste und Popupmeldungen).

SIEHE AUCH

Aktive Elemente der Benutzeroberfläche 187

Grafische Oberfläche von Kaspersky Internet Security 188

AKTIVE ELEMENTE DER BENUTZEROBERFLÄCHE

Um die aktiven Elemente der Benutzeroberfläche anzupassen (z.B. Symbol von Kaspersky Internet Security in der Taskleiste und Popupmeldungen), stehen folgende Möglichkeiten zur Verfügung:

Animation des Symbols bei Aufgabenausführung verwenden.

In Abhängigkeit von der ausgeführten Programmaktion ändert sich das Symbol im Infobereich. Wird beispielsweise die Untersuchung eines Skripts ausgeführt, dann erscheint im Hintergrund des Symbols ein kleines Piktogramm mit einem Skript. Bei der Untersuchung einer E-Mail-Nachricht erscheint das Piktogramm eines Briefs. Das Symbol von Kaspersky Internet Security wird animiert. Es gibt in diesem Fall nur den Schutzstatus Ihres Computers wieder: Wenn der Schutz aktiviert ist, ist das Symbol farbig. Wenn der Schutz angehalten oder ausgeschaltet wurde, ist es grau.

Transparenz für Meldungsfenster verwenden.

Alle Operationen des Programms, die Ihre sofortige Aufmerksamkeit oder Entscheidung erfordern, besitzen das Aussehen einer Popupmeldung die über dem Programmsymbol im Infobereich erscheinen. Die Meldungsfenster sind halbtransparent, damit sie Ihre Arbeit nicht stören. Wenn der Mauscursor auf das Meldungsfenster geführt wird, wird die Transparenz aufgehoben.

Über Neuigkeiten benachrichtigen.

Standardmäßig erscheint beim Eintreffen von Nachrichten in der Taskleiste ein spezielles Symbol. Durch Klick auf das Symbol wird ein Fenster mit dem Nachrichtentext geöffnet.

"Protected by Kaspersky Lab" über dem Microsoft Windows-Begrüßungsbildschirm anzeigen.

Dieser Indikator erscheint in der Grundeinstellung rechts oben am Bildschirmrand, wenn Kaspersky Internet Security gestartet wird. Er informiert darüber, dass der Schutz Ihres Computers vor jeder Art von Bedrohung aktiviert ist.

Wenn der Computer, auf dem das Programm installiert ist, ein Betriebssystem der Produktfamilie Microsoft Windows Vista verwendet, steht diese Option nicht zur Verfügung.

Gehen Sie folgendermaßen vor, um die aktiven Elemente der Benutzeroberfläche anzupassen:

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
2. Wählen Sie im folgenden Fenster den Abschnitt **Ansicht**.
3. Aktivieren oder deaktivieren Sie im Block **Symbol in der Taskleiste** die entsprechenden Kontrollkästchen.

GRAFISCHE OBERFLÄCHE VON KASPERSKY INTERNET SECURITY

Alle auf der Oberfläche von Kaspersky Internet Security verwendeten Farben, Schriften, Piktogramme und Texte können verändert werden. Sie können eine individuelle grafische Oberfläche für das Programm erstellen und es in einer anderen Sprache lokalisieren.

Gehen Sie folgendermaßen vor, um eine andere grafische Oberfläche zu verwenden:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie im folgenden Fenster den Abschnitt **Ansicht**.
3. Aktivieren Sie im Block **Grafische Oberflächen** das Kontrollkästchen **Alternative Programmoberfläche verwenden**, um eine grafische Oberfläche einzubinden. Geben Sie im Eingabefeld den Ordner mit den Parametern der grafischen Oberfläche an. Klicken Sie zur Auswahl eines Ordners auf die Schaltfläche **Durchsuchen**.

PROFILE FÜR KASPERSKY INTERNET SECURITY VERWENDEN

Wenn bestimmte Programme (z.B. Spiele) im Vollbildmodus verwendet werden, kann es erforderlich sein, einzelne Funktionen von Kaspersky Internet Security (insbesondere den Benachrichtigungsdienst) zu deaktivieren. Solche Programme sind oft sehr ressourcenaufwändig und deshalb könnte die gleichzeitige Ausführung bestimmter Aufgaben von Kaspersky Internet Security zur Verlangsamung ihrer Arbeit führen.

Damit der Benutzer nicht jedes Mal, wenn er Vollbild-Anwendungen einsetzt, manuell die Benachrichtigungen ausschalten und Aufgaben anhalten muss, bietet Kaspersky Internet Security die Möglichkeit, diese Parameter mit Hilfe eines Profils für Spiele vorübergehend zu ändern. Das Profil für Spiele erlaubt es, beim Wechsel in den Vollbildmodus gleichzeitig die Parameter aller Komponenten zu ändern und beim Verlassen des Vollbildmodus die vorgenommenen Änderungen wieder rückgängig zu machen.

Die Ereignisbenachrichtigungen werden beim Wechsel in den Vollbildmodus automatisch deaktiviert. Außerdem können folgende Parameter angegeben werden:

- **Aktion automatisch auswählen**. Bei Auswahl dieser Variante wird als Reaktion für alle Komponenten die automatische Auswahl einer Aktion verwendet, selbst wenn in ihren Einstellungen die Variante **Aktion erfragen** festgelegt wurde. Auf diese Weise wird der Benutzer beim Fund von Bedrohungen nicht nach einer Aktion gefragt, sondern das Programm wählt automatisch eine Aktion aus.

- **Update nicht ausführen** und **Geplante Untersuchungsaufgaben nicht starten**. Es wird empfohlen, diese Parameter zu verwenden, um eine Verlangsamung von Vollbild-Anwendungen zu vermeiden.

Gehen Sie folgendermaßen vor, um die Verwendung des Profils für Spiele zu aktivieren:

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.

2. Wählen Sie im folgenden Fenster den Abschnitt **Profil für Spiele**.

3. Aktivieren Sie das Kontrollkästchen **Profil für Spiele aktivieren** und geben Sie die entsprechenden Parameter an.

ZUSÄTZLICHE OPTIONEN

Es ist eine schwierige Aufgabe, die Sicherheit eines Computers zu gewährleisten. Dafür sind Kenntnisse über Besonderheiten der Funktion eines Betriebssystems und über potentielle Schwachstellen erforderlich. Zudem erschweren die große Menge und die Vielfalt der Informationen über die Systemsicherheit deren Analyse und Verarbeitung.

Um spezifische Aufgaben, die die Sicherheit des Computers gewährleisten, zu vereinfachen, verfügt Kaspersky Internet Security über unterschiedliche Assistenten und Werkzeuge.

- Virtuelle Tastatur (s. S. 190, sodass keine über die Tastatur eingegebenen Daten erfasst werden können.
- Die Programmkomponente Kindersicherung (s. S. 191) kontrolliert den Zugriff von Computerbenutzern auf Webressourcen.
- Der Assistent zum Erstellen einer Notfall-CD (s. S. 191) dient dazu, die Funktionsfähigkeit des Systems nach einem Virenangriff wiederherzustellen, wenn Systemdateien des Betriebssystems beschädigt wurden und der Computer nicht mehr hochgefahren werden kann.
- Der Assistent zur Browser-Konfiguration (s. S. 194) führt eine Analyse der Einstellungen des Browsers Microsoft Internet Explorer aus. Dabei werden die Einstellungen hauptsächlich im Hinblick auf die Sicherheit bewertet.
- Die Analyse von Netzwerkpaketen (s. S. 195) fängt Netzwerkpakete ab und bietet ausführliche Informationen darüber.
- Der Assistent zur Wiederherstellung nach einer Infektion (s. S. 196) beseitigt im System die Spuren von schädlichen Objekten.
- Der Assistent zum Löschen von Aktivitätsspuren (s. S. 197) sucht und beseitigt im System die Aktivitätsspuren des Benutzers.

IN DIESEM ABSCHNITT

Virtuelle Tastatur 190

Kindersicherung 191

Notfall-CD 191

Browser-Konfiguration 194

Analyse von Netzwerkpaketen 195

Wiederherstellung nach Infektion 196

Assistent zum Löschen von Aktivitätsspuren 197

Netzwerkmonitor 198

VIRTUELLE TASTATUR

Bei der Arbeit auf einem Computer ist es häufig erforderlich, persönliche Daten, Benutzername und Kennwort einzugeben. Beispiele sind die Anmeldung auf Internetseiten, der Besuch von Online-Shops usw.

In solchen Situationen besteht die Gefahr, dass persönliche Informationen mit Hilfe von Hardware-Hooks oder mit Keyloggern (Programme, die Tasteneingaben registrieren) abgefangen werden.

Die virtuelle Tastatur ermöglicht es, das Abfangen von, über die Tastatur eingegebenen, Daten zu verhindern.

Die virtuelle Tastatur kann Ihre persönlichen Daten nicht schützen, wenn eine Webseite gehackt wurde und die Eingabe solcher Daten fordert, weil die Informationen in diesem Fall dem Angreifer direkt in die Hände fallen.

Viele Spyware-Programme besitzen Funktionen zum Anlegen von Screenshots, die an Angreifer für Analyse und Sammeln von persönlichen Benutzerdaten automatisch übergeben werden. Die virtuelle Tastatur schützt die eingegebenen persönlichen Daten, die durch das Anlegen von Screenshots abgefangen werden können.

Die virtuelle Tastatur schützt persönliche Daten nur dann vor Diebstahlversuchen, wenn Sie mit den Internetbrowsern Microsoft Internet Explorer und Mozilla Firefox arbeiten.

➡ *Gehen Sie folgendermaßen vor, um die virtuelle Tastatur zu verwenden:*

1. Öffnen Sie das Programmhauptfenster.
2. Wählen Sie auf der linken Fensterseite den Abschnitt **Sicherheit+** und klicken Sie auf die Schaltfläche **Virtuelle Tastatur**.
3. Geben Sie die erforderlichen Daten über die virtuelle Tastatur ein. Vergewissern Sie sich, dass die Daten im erforderlichen Feld eingegeben wurden. Die Funktionstasten (**Umschalt** , **Alt** , **Strg**) der virtuellen Tastatur verfügen über eine Einrastfunktion (wenn beispielsweise die **Umschalt**-Taste einmal angeklickt wurde, werden alle Zeichen groß geschrieben). Um die Einrastfunktion aufzuheben, klicken Sie erneut auf die Funktionstaste.

KINDERSICHERUNG

Die Programmkomponente *Kindersicherung* kontrolliert den Zugriff von Computerbenutzern auf Webressourcen. Die Hauptaufgabe der Kindersicherung besteht darin, den Zugriff auf folgende Ressourcen zu beschränken:

- Webseiten, die für Erwachsene bestimmt sind, oder Webseiten, die Themen wie Pornografie, Waffen, Drogen betreffen oder Grausamkeit, Gewalt usw. provozieren.
- Webseiten, die Zeitverlust (Chats, Glücksspiele) oder Geldverlust (Online-Shops, Auktionen) verursachen können.

Solche Webseiten enthalten häufig mehrere Schadprogramme. Außerdem verursacht der Download von Daten aus Ressourcen wie beispielsweise Spielseiten eine bedeutende Erhöhung des Internet-Datenverkehrs.

Die Kindersicherung (s. S. 126) ist nach der Installation von Kaspersky Internet Security deaktiviert.

NOTFALL-CD

Kaspersky Internet Security enthält einen Dienst zum Erstellen einer Notfall-CD.

Die Notfall-CD dient zur Untersuchung und Desinfektion infizierter x86-kompatibler Computer. Sie kommt dann zum Einsatz, wenn der Infektionsgrad so hoch ist, dass die Desinfektion eines Computers nicht mehr mit Hilfe von Antiviren-Anwendungen oder Desinfektionstools (z.B. Kaspersky AVPTool) möglich ist, die unter dem Betriebssystem gestartet werden. Dabei wird die Effektivität der Desinfektion gesteigert, weil die im System vorhandenen Schädlinge nicht die Kontrolle übernehmen können, während das Betriebssystem hochgefahren wird.

Eine Notfall-CD wird auf Basis eines Linux-Betriebssystemkerns erstellt und ist eine ISO-Datei, die folgende Elemente umfasst:

- System- und Konfigurationsdateien für Linux.
- eine Auswahl von Tools zur Betriebssystemdiagnose

- Auswahl von sonstigen Utilities (Datei-Manager u.a.).
- Dateien für Kaspersky Rescue Disk.
- Dateien, die die Antiviren-Datenbanken enthalten.

Ein Computer, dessen Betriebssystem beschädigt ist, wird über das CD / DVD-ROM-Laufwerk hochgefahren. Dafür muss auf dem Computer ein entsprechendes Gerät installiert sein.

Gehen Sie folgendermaßen vor, um eine Notfall-CD zu erstellen:

1. Öffnen Sie das Programmhauptfenster.
2. Wählen Sie auf der linken Fensterseite den Abschnitt **Sicherheit+**.
3. Klicken Sie auf die Schaltfläche **Notfall-CD**, um den Assistenten für die Notfall-CD zu starten.
4. Folgen Sie den Anweisungen des Assistenten.
5. Verwenden Sie die Datei, die mit Hilfe des Assistenten erstellt wurde, um eine Bootdisk (CD/DVD) zu brennen. Dafür kann ein Brennprogramm für CDs / DVDs (z.B. Nero) eingesetzt werden.

SIEHE AUCH

Notfall-CD erstellen 192

Hochfahren eines Computers mit Hilfe der Notfall-CD 193

NOTFALL-CD ERSTELLEN

Das Anlegen einer Notfall-CD umfasst das Erstellen eines Disk-Abbild (ISO-Datei) mit den aktuellen Programm-Datenbanken und Konfigurationsdateien.

Ein Original des Disk-Abbilds, auf dessen Basis eine neue Datei erstellt wird, kann von einem Kaspersky-Lab-Server heruntergeladen oder aus einer lokalen Quelle kopiert werden.

Die Abbild-Datei, die vom Assistenten erstellt wurde, wird unter dem Namen *rescuecd.iso* im Ordner "*Dokumente und Einstellungen\All Users\Anwendungsdaten\Kaspersky Lab\AVP9\Data\Rdisk*" ("*ProgramData\Kaspersky Lab\AVP9\Data\Rdisk*\" – für Microsoft Vista) abgelegt. Wenn der Assistent im angegebenen Ordner eine früher erstellte Abbild-Datei gefunden hat, aktivieren Sie das Kontrollkästchen **Vorhandenes Abbild verwenden**. Sie können die Datei als Basis für das Disk-Abbild verwenden und sofort mit Schritt 3 (Abbild aktualisieren) fortfahren. Wenn der Assistent keine Abbild-Datei gefunden hat, fehlt dieses Kontrollkästchen.

Die Notfall-CD wird mit Hilfe eines Assistenten erstellt, der aus einer Reihe von Fenstern (Schritten) besteht. Zur Navigation zwischen den Fenstern dienen die Schaltflächen **Zurück** und **Weiter**, zum Abschluss des Assistenten die Schaltfläche **Beenden**. Die Arbeit des Assistenten kann auf einer beliebigen Etappe durch Klick auf die Schaltfläche **Abbrechen** beendet werden.

SIEHE AUCH

Notfall-CD 191

Hochfahren eines Computers mit Hilfe der Notfall-CD 193

HOCHFAHREN EINES COMPUTERS MIT HILFE DER NOTFALL-CD

Wenn sich das Betriebssystem aufgrund eines Virenangriffs nicht mehr hochfahren lässt, können Sie die Notfall-CD einsetzen.

Um das Betriebssystem hochzufahren, ist eine Abbild-Datei (.iso) der Notfall-CD erforderlich. Sie können die Datei von einem Kaspersky-Lab-Server herunterladen oder eine vorhandene Datei aktualisieren.

Im Folgenden wird die Arbeit der Notfall-CD ausführlich erläutert. Während des Downloads der Datei finden folgende Operationen statt:

1. Die Hardware des Computers wird automatisch ermittelt.
2. Auf den Festplatten wird nach Dateisystemen gesucht. Gefundene Dateisysteme erhalten einen Namen, der mit *C* beginnt.

   Die Namen, die den Festplatten und Wechselmedien zugewiesen werden, können von ihren Namen im Betriebssystem abweichen.

   Wenn sich das Betriebssystem des Computers, der hochgefahren werden soll, im Ruhezustand befindet oder das Dateisystem den Status *unclean* besitzt, weil beim Herunterfahren ein Fehler aufgetreten ist, können Sie entscheiden, ob das Dateisystem gemountet oder der Computer neu gestartet werden soll.

   Das Mounten des Dateisystems kann zu seiner Beschädigung führen.
3. Die Auslagerungsdatei von Microsoft Windows *pagefile.sys* wird gesucht. Wenn sie nicht vorhanden ist, wird die Größe des virtuellen Speichers durch die Größe des Arbeitsspeichers begrenzt.
4. Eine Sprache wird ausgewählt. Wenn innerhalb einer bestimmten Zeit keine Auswahl stattfindet, wird standardmäßig die Sprache Englisch gewählt.
5. Es werden Ordner zum Speichern von Antiviren-Datenbanken, Berichten, Quarantäne und sonstigen Dateien gesucht (erstellt). In der Grundeinstellung werden die Ordner des Kaspersky-Lab-Programms verwendet, das auf dem infizierten Computer installiert ist (*„ProgramData/Kaspersky Lab/AVP9“* – für Microsoft Windows Vista, *“Dokumente und Einstellungen/All Users/Anwendungsdaten/Kaspersky Lab/AVP9“* – für ältere Versionen von Microsoft Windows). Wenn diese Ordner des Programms nicht gefunden werden, wird versucht, sie zu erstellen. Falls die Ordner nicht gefunden wurden und nicht erstellt werden können, wird auf einem der Laufwerke der Ordner *kl.files* erstellt.
6. Es wird versucht, mit Hilfe der Daten, die in den Systemdateien des hochzufahrenden Computers gefunden werden, die Netzwerkverbindungen anzupassen.
7. Das grafische Subsystem wird geladen und Kaspersky Rescue Disk wird gestartet.

Im Rettungsmodus sind nur die Aufgaben zur Virensuche und zum Update der Datenbanken aus einer lokalen Quelle verfügbar, sowie das Rollback für Updates und die Anzeige der Statistik.

➡ *Gehen Sie folgendermaßen vor, um das Betriebssystem des infizierten Computers hochzufahren:*

1. Wählen Sie in den BIOS-Einstellungen das Booten von CD/DVD-ROM (weitere Informationen können der Dokumentation zum Motherboard Ihres Computers entnommen werden).
2. Legen Sie die Disk, auf die das Disk-Abbild gebrannt wurde, in das CD/DVD-Laufwerk des infizierten Computers ein.
3. Starten Sie den Computer neu.

Danach wird der Computer nach dem oben beschriebenen Algorithmus hochgefahren. Ausführliche Informationen über die Funktionen der Notfall-CD gibt die Hilfe zu Kaspersky Rescue Disk.

SIEHE AUCH

Notfall-CD 191

Notfall-CD erstellen 192

BROWSER-KONFIGURATION

Der Assistent zur Browser-Konfiguration führt eine Analyse der Einstellungen des Browsers Microsoft Internet Explorer aus. Dabei werden die Einstellungen vorrangig im Hinblick auf die Sicherheit bewertet, weil bestimmte benutzerdefinierte oder standardmäßige Parameter zu Sicherheitsproblemen führen können.

Der Assistent prüft, ob die aktuellen Updates für den Browser installiert sind und ob seine Einstellungen potentielle Schwachstellen aufweisen, die von Angreifern ausgenutzt werden können, um Ihrem Computer zu beschädigen. Beispiele für zu untersuchenden Objekte:

- **Cache des Microsoft Internet Explorer**. Der Zwischenspeicher enthält vertrauliche Daten und kann außerdem Aufschluss darüber geben, welche Ressourcen der Benutzer besucht hat. Viele schädliche Objekte lesen beim Scannen der Festplatte auch den Zwischenspeicher. Auf diese Weise können Angreifer die Mailadressen von Benutzern erhalten. Es wird empfohlen, den Zwischenspeicher zu leeren, wenn die Arbeit mit dem Browser beendet wird.

- **Anzeige von Erweiterungen für das System bekannte Dateitypen**. Für Benutzer ist es vorteilhaft, die tatsächliche Dateierweiterung zu sehen. Viele schädliche Objekte verwenden eine doppelte Erweiterung. In diesem Fall sieht der Benutzer nur einen Teil des Dateinamens, nicht aber die tatsächliche Erweiterung. Diese Methode wird häufig von Angreifern benutzt. Es wird empfohlen, die Anzeige von Erweiterungen für Dateien bekannter Formate zu aktivieren.

- **Liste mit vertrauenswürdigen Seiten**. Schädliche Objekte können einer solchen Liste Links zu Seiten, die von Angreifern erstellt wurden, hinzufügen.

Schließen Sie alle Browserfenster von Microsoft Internet Explorer, bevor mit der Diagnose begonnen wird.

Nach der Untersuchung analysiert der Assistent die gesammelten Informationen, um festzustellen, ob in den Einstellungen des Browsers Sicherheitsprobleme vorliegen, die sofort behoben werden müssen. Das Ergebnis der Untersuchung besteht in einer Liste von Aktionen, die ausgeführt werden sollten, um die Probleme zu beheben. Die Aktionen sind nach der Priorität der gefundenen Probleme in Kategorien angeordnet.

Beim Abschluss des Assistenten wird ein Bericht erstellt, der zur Analyse an Kaspersky Lab geschickt werden kann.

Es sollte berücksichtigt werden, dass bestimmte Einstellungen zu Problemen bei der Anzeige spezieller Seiten führen können (beispielsweise wenn sie ActiveX-Elemente verwenden). Das Problem lässt sich lösen, indem solche Seiten in die vertrauenswürdige Zone aufgenommen werden.

Der Assistent besteht aus einer Reihe von Fenstern (Schritten). Zur Navigation zwischen den Fenstern dienen die Schaltflächen **Zurück** und **Weiter**, zum Abschluss des Assistenten die Schaltfläche **Beenden**. Die Arbeit des Assistenten kann auf einer beliebigen Etappe durch Klick auf die Schaltfläche **Abbrechen** beendet werden.

Gehen Sie folgendermaßen vor, den Assistenten zu starten:

1. Öffnen Sie das Programmhauptfenster.

2. Wählen Sie auf der linken Fensterseite den Abschnitt **Sicherheit+** und klicken Sie auf die Schaltfläche **Browser-Konfiguration**.

ANALYSE VON NETZWERKPAKETEN

Das Werkzeug **Analyse von Netzwerkpaketen** ist für erfahrene Anwender gedacht, die sich mit der Struktur von Netzwerken und Netzwerkprotokollen auskennen.

Kaspersky Internet Security bietet das Werkzeug *Analyse von Netzwerkpaketen*. Dieses Werkzeug dient zum Sammeln und zur Analyse der Netzwerkaktivität im Netzwerk, zu dem Ihr Computer gehört.

Die Analyse von Netzwerkpaketen fängt nach ihren Start alle Pakete, die über ein Netzwerk übertragen werden, ab. Die Anzahl der abgefangenen Pakete kann sehr groß sein. Um die Analyse der gesammelten Informationen zu erleichtern, können Sie die Filterung eines Pakets nach Ursprungs- und Zieladressen (s. S. 196) und nach dem Übertragungsprotokoll (s. S. 196) verwenden.

Die Analyse von Netzwerkpaketen steht nach der Installation von Kaspersky Internet Security nicht im Programmhauptfenster zu Verfügung. Vor dem Beginn der Arbeit mit der Analyse von Netzwerkpaketen ist es erforderlich, den Zugriff darauf zu öffnen (s. S. 195).

Gehen Sie folgendermaßen vor, um die Analyse von Netzwerkpaketen zu starten:

1. Öffnen Sie das Programmhauptfenster.
2. Wählen Sie auf der linken Fensterseite den Abschnitt **Sicherheit+** und klicken Sie auf die Schaltfläche **Analyse von Netzwerkpaketen**.

SIEHE AUCH

Zugriff auf die Analyse von Netzwerkpaketen .....

Überwachung von Paketen starten / beenden .....

Paketfilterung nach Ursprungs- und Zieladressen .....

Paketfilterung nach Übertragungsprotokoll .....

ZUGRIFF AUF DIE ANALYSE VON NETZWERKPAKETEN

Die Analyse von Netzwerkpaketen steht in der Grundeinstellung nicht im Hauptfenster von Kaspersky Internet Security zur Verfügung.

Gehen Sie folgendermaßen vor, um den Zugriff auf die Analyse von Netzwerkpaketen zu öffnen:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie im folgenden Fenster den Abschnitt **Netzwerk** aus und aktivieren Sie im Block **Analyse von Netzwerkpaketen** das Kontrollkästchen **Monitor "Analyse von Netzwerkpaketen" anzeigen**.

ÜBERWACHUNG VON PAKETEN STARTEN / BEENDEN

Die Analyse von Netzwerkpaketen funktioniert auf der Grundlage einer Statistik, die sich aus abgefangenen Paketen ergibt.

Gehen Sie folgendermaßen vor, um die Überwachung von Paketen zu starten:

1. Öffnen Sie das Programmhauptfenster.

2. Wählen Sie auf der linken Fensterseite den Abschnitt **Sicherheit+** und klicken Sie auf die Schaltfläche **Analyse von Netzwerkpaketen**.

3. Klicken Sie im folgenden Fenster **Statistik zur Analyse von Netzwerkpaketen** auf die Schaltfläche **Start**. Es ist erst nach dem Beenden der Paketüberwachung möglich, gesammelte Daten zu filtern und das Fenster der Analyse von Netzwerkpaketen zu schließen.

PAKETFILTERUNG NACH URSPRUNGS- UND ZIELADRESSEN

Die große Menge von Informationen, die von der Analyse von Netzwerkpaketen gesammelt wird, erschwert ihre Verarbeitung und Analyse. Um die Analyse der Information zu erleichtern, kann die Filterung nach Ursprungs- und Zieladressen von Paketen verwendet werden.

Gehen Sie folgendermaßen vor, um die Paketfilterung nach Ursprungs- und Zieladressen zu verwenden:

1. Öffnen Sie das Programmhauptfenster.

2. Wählen Sie auf der linken Fensterseite den Abschnitt **Sicherheit+** und klicken Sie auf die Schaltfläche **Analyse von Netzwerkpaketen**.

3. Klicken Sie im folgenden Fenster **Statistik zur Analyse von Netzwerkpaketen** auf die Schaltfläche **Start**.

4. Geben Sie in den Feldern **Quelle** und **Ziel** die erforderlichen IP-Adressen an und klicken Sie im oberen Bereich des Fensters auf die Schaltfläche **Filtern**. Die Ergebnisse der Filterung werden auf der linken Seite des Fensters angezeigt.

   Um die Filterung aufzuheben, löschen Sie die Werte in den Feldern **Quelle** und **Ziel** und klicken im oberen Bereich des Fensters Sie auf die Schaltfläche **Filtern**. Die von der Aktivitätsanalyse gesammelten Daten werden erneut so dargestellt wie zum Zeitpunkt, als die Paketüberwachung beendet wurde.

PAKETFILTERUNG NACH ÜBERTRAGUNGSPROTOKOLL

Die große Menge von Informationen, die von der Analyse von Netzwerkpaketen gesammelt wird, erschwert ihre Verarbeitung und Analyse. Um die Analyse der Information zu erleichtern, kann die Filterung nach dem Übertragungsprotokoll von Paketen verwendet werden.

Gehen Sie folgendermaßen vor, um die Paketfilterung nach dem Übertragungsprotokoll zu verwenden:

1. Öffnen Sie das Programmhauptfenster.

2. Wählen Sie auf der linken Fensterseite den Abschnitt **Sicherheit+** und klicken Sie auf die Schaltfläche **Analyse von Netzwerkpaketen**.

3. Klicken Sie im folgenden Fenster **Statistik zur Analyse von Netzwerkpaketen** auf die Schaltfläche **Start**.

4. Wählen Sie in der Dropdown-Liste **Protokoll** das entsprechende Protokoll aus und klicken Sie im oberen Bereich des Fensters auf die Schaltfläche **Filtern**. Die Ergebnisse der Filterung werden auf der linken Seite des Fensters angezeigt.

   Um die Filterung aufzuheben, wählen Sie in der Dropdown-Liste **Protokoll** den leeren Wert aus und klicken Sie im oberen Bereich des Fensters auf die Schaltfläche **Filtern**. Die von der Aktivitätsanalyse gesammelten Daten werden erneut so dargestellt wie zum Zeitpunkt, als die Paketüberwachung beendet wurde.

WIEDERHERSTELLUNG NACH INFEKTION

Der Assistent zur Wiederherstellung nach einer Infektion beseitigt im System die Spuren von schädlichen Objekten. Die Kaspersky-Lab-Spezialisten empfehlen, den Assistenten nach der Desinfektion des Computers zu starten, um sicherzustellen, dass alle Bedrohungen und die von ihnen verursachten Beschädigungen beseitigt werden. Der Assistent kann auch verwendet werden, wenn der Verdacht auf eine Infektion eines Computers besteht.

Der Assistent prüft, ob im System Veränderungen vorliegen. Dazu zählen z.B.: blockierter Zugriff auf die Netzwerkumgebung, veränderte Dateierweiterungen bekannter Formate, blockierte Systemsteuerung usw. Mögliche Gründe für das Auftreten solcher Beschädigungen sind die Aktivität schädlicher Programme, Systemabstürze sowie die Verwendung inkorrekt funktionierender Systemoptimierungsprogramme.

Nach der Untersuchung analysiert der Assistent die gesammelten Informationen, um festzustellen, ob im System Beschädigungen vorliegen, die sofort behoben werden müssen. Das Ergebnis der Untersuchung besteht in einer Liste von Aktionen, die ausgeführt werden sollten, um die Beschädigungen zu beheben. Die Aktionen sind nach der Priorität der gefundenen Probleme in Kategorien angeordnet.

Der Assistent besteht aus einer Reihe von Fenstern (Schritten). Zur Navigation zwischen den Fenstern dienen die Schaltflächen **Zurück** und **Weiter**, zum Abschluss des Assistenten die Schaltfläche **Beenden**. Die Arbeit des Assistenten kann auf einer beliebigen Etappe durch Klick auf die Schaltfläche **Abbrechen** beendet werden.

Gehen Sie folgendermaßen vor, den Assistenten zu starten:

1. Öffnen Sie das Programmhauptfenster.
2. Wählen Sie auf der linken Fensterseite den Abschnitt **Sicherheit+** und klicken Sie auf die Schaltfläche **Wiederherstellung nach Infektion**.

ASSISTENT ZUM LÖSCHEN VON AKTIVITÄTSSPUREN

Während der Arbeit auf dem Computer werden die Aktionen des Benutzers im System registriert. Dabei werden folgende Daten gespeichert:

- Verlauf mit Informationen über:
  - besuchte Webseiten.
  - den Start von Programmen
  - Suchanfragen.
  - das Öffnen / Speichern von Dateien mit bestimmten Anwendungen.
- Einträge im Systembericht von Microsoft Windows
- temporäre Dateien u.a.

Alle genannten Informationsquellen über die Benutzeraktivität können sensible Daten wie z.B. Kennwörter enthalten und von Angreifern analysiert werden. Allerdings verfügt der Benutzer häufig nicht über ausreichende Kenntnisse, um dieser Methode des Diebstahls wertvoller Informationen vorzubeugen.

Kaspersky Internet Security verfügt über einen **Assistenten zum Löschen von Aktivitätsspuren**. Dieser Assistent führt im System die Suche nach Spuren von Benutzeraktivität und den Betriebssystemparametern, die zum Sammeln von Informationen über die Aktivität dienen, durch.

Es werden laufend Informationen über die Aktivität des Benutzers im System gesammelt. Der Start einer beliebigen Datei oder das Öffnen eines Dokuments werden in einem Verlauf festgehalten, und das Systemjournal von Microsoft Windows registriert eine Vielzahl von Ereignissen, die im System vorfallen. Deshalb kann es sein, dass bei einem wiederholten Start des Assistenten zum **Löschen von Aktivitätsspuren** gefunden werden, die beim vorhergehenden Start des Assistenten bereits gelöscht worden sind. Bestimmte Dateien wie z.B. eine Journaldatei von Microsoft Windows können vom System verwendet werden, während sie vom Assistenten gelöscht werden sollen. Um diese Dateien zu löschen, schlägt der Assistent vor, das System neu zu starten. Im Verlauf eines Neustarts können solche Dateien aber erneut erstellt werden, was dazu führt, dass sie wieder als Aktivitätsspuren erkannt werden.

Der Assistent besteht aus einer Reihe von Fenstern (Schritten). Zur Navigation zwischen den Fenstern dienen die Schaltflächen **Zurück** und **Weiter**, zum Abschluss des Assistenten die Schaltfläche **Beenden**. Die Arbeit des Assistenten kann auf einer beliebigen Etappe durch Klick auf die Schaltfläche **Abbrechen** beendet werden.

Gehen Sie folgendermaßen vor, den Assistenten zu starten:

1. Öffnen Sie das Programmhauptfenster.

2. Wählen Sie auf der linken Fensterseite den Abschnitt **Sicherheit+** und klicken Sie auf die Schaltfläche **Löschen von Aktivitätsspuren**.

NETZWERKMONITOR

Der *Netzwerkmonitor* dient dazu, in Echtzeit Informationen über die Netzwerkaktivität anzuzeigen. Um den Netzwerkmonitor zu starten, verwenden Sie den gleichnamigen Befehl im Kontextmenü.

Das folgende Fenster enthält folgende Registerkarten:

- Auf der Registerkarte *Verbindungen und Ports* werden alle offenen Ports und aktiven Netzwerkverbindungen, die momentan auf Ihrem Computer bestehen, angezeigt.

- Die Registerkarte *Firewall: Journal über Regelverarbeitung* enthält Informationen über die Verwendung von Paketregeln für Programme.

- Die Registerkarte *Netzwerkverkehr* enthält Informationen über alle ein- und ausgehenden Verbindungen, die zwischen Ihrem Computer und anderen Computern (einschließlich Webservern, Mailservern usw.) aufgebaut werden.

- Die Registerkarte *Blockierte Computer* enthält eine Liste der blockierten Computer.

BERICHTE

Die Arbeit jeder Komponente von Kaspersky Internet Security und die Ausführung jeder Untersuchungs- und Updateaufgabe werden in einem Bericht protokolliert.

Bei der Arbeit mit Berichten können Sie folgende Aktionen ausführen:

- Komponente / Aufgabe auswählen (s. S. 199), für die ein Ereignisbericht angezeigt werden soll.
- Datengruppierungen verwalten (s. S. 200) und deren Bildschirmanzeige (s. S. 202).
- Zeitplan erstellen (s. S. 200), nach dem Kaspersky Internet Security Sie über die Bereitschaft eines Berichts benachrichtigen soll.
- auswählen, für welchen Ereignistyp (s. S. 201) ein Bericht erstellt werden soll.
- auswählen, in welcher Form die statistischen Informationen auf dem Bildschirm dargestellt werden sollen - als Tabelle oder Grafik (s. S. 203).
- Bericht in einer Datei speichern (s. S. 204).
- komplexe Filterbedingungen (s. S. 204) festlegen.
- Suche nach Ereignissen (s. S. 205) organisieren, die im System eingetreten und vom Programm verarbeitet wurden.

IN DIESEM ABSCHNITT

Komponente oder Aufgabe für das Erstellen eines Berichts auswählen 199

Anordnung von Informationen im Bericht 200

Über Bereitschaft des Berichts benachrichtigen 200

Ereignistyp auswählen 201

Darstellung von Daten auf dem Bildschirm 202

Darstellung der Statistik als Tabelle oder Grafik 203

Bericht in Datei speichern 204

Verwendung der komplexen Filterung 204

Suche nach Ereignissen 205

KOMPONENTE ODER AUFGABE FÜR DAS ERSTELLEN EINES BERICHTS AUSWÄHLEN

Sie können Informationen über die Ereignisse erhalten, die bei der Arbeit der einzelnen Komponenten von Kaspersky Internet Security oder bei der Ausführung von Aufgaben (z.B. Datei-Anti-Virus, Update usw.) eingetreten sind.

Gehen Sie folgendermaßen vor, um einen Bericht über eine bestimmte Komponente oder Aufgabe zu erhalten:

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Bericht**.
2. Klicken Sie im folgenden Fenster auf der Registerkarte **Bericht** auf die Schaltfläche **Vollständiger Bericht**.
3. Wählen Sie im folgenden Fenster links in der Dropdown-Liste eine Komponente oder eine Aufgabe aus, für die ein Bericht erstellt werden soll. Bei Auswahl des Punkts **Schutz-Center** wird ein Bericht für alle Schutzkomponenten erstellt.

ANORDNUNG VON INFORMATIONEN IM BERICHT

Sie können die Anordnung der im Bericht enthaltenen Daten steuern. Die Informationen können nach unterschiedlichen Merkmalen sortiert werden. Die Auswahl der Merkmale ist für jede Komponente und Aufgaben individuell. Folgende Varianten stehen zur Auswahl:

- **Unsortiert**. Alle Ereignisse werden angezeigt.
- **Nach Aufgabe anordnen**. Die Daten werden nach den Aufgaben, die von den Komponenten von Kaspersky Internet Security ausgeführt wurden, angeordnet.
- **Nach Programm anordnen**. Die Daten werden nach Programmen angeordnet, die im System aktiv waren und von Kaspersky Internet Security verarbeitet wurden.
- **Nach Untersuchungsergebnis anordnen**. Die Daten werden nach den Ergebnissen der Untersuchung oder Verarbeitung eines Objekts angeordnet.

Abbildung 13: Gruppierungskennzeichen für Berichtsdaten

Zur Vereinfachung und Verkleinerung der Gruppierung ist eine Suche (s. Abschnitt "Suche nach Ereignissen" auf S. 205) nach einem Schlüsselwort vorgesehen. Außerdem können Sie die Suchkriterien festlegen.

Gehen Sie folgendermaßen vor, um die Anordnung nach einen bestimmten Merkmal zu verwenden:

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Bericht**.
2. Klicken Sie im folgenden Fenster auf der Registerkarte **Bericht** auf die Schaltfläche **Vollständiger Bericht**.
3. Wählen Sie im folgenden Fenster in der Dropdown-Liste ein Anordnungsmerkmal aus.

ÜBER BEREITSCHAFT DES BERICHTS BENACHRICHTIGEN

Sie können einen Zeitplan erstellen, nach dem Kaspersky Internet Security Sie über die Bereitschaft eines Berichts benachrichtigen soll.

Gehen Sie folgendermaßen vor, um einen Zeitplan für das Senden von Benachrichtigungen zu erstellen:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Bericht** im oberen Bereich des Fensters.
2. Im folgenden Fenster auf der Registerkarte **Bericht** aktivieren Sie das Kontrollkästchen **An Bericht erinnern**. Klicken Sie auf den Link mit dem festgelegten Zeitpunkt.
3. Im nächsten Fenster **Bericht: Zeitplan** legen Sie einen Zeitplan an.

EREIGNISTYP AUSWÄHLEN

Eine vollständige Liste aller wichtigen Ereignisse, die bei der Arbeit einer Schutzkomponente, beim Ausführen einer Untersuchungsaufgabe oder beim Update der Programm-Datenbanken eintreten, wird in einem Bericht aufgezeichnet. Sie können den Typ der Ereignisse auswählen, die im Bericht angezeigt werden sollen.

Es gibt folgende Ereignistypen:

- *Kritische Ereignisse*. Ereignisse mit kritischer Priorität, die auf Probleme bei der Arbeit von Kaspersky Internet Security oder auf Schwachstellen im Schutz Ihres Computers hinweisen. Dazu zählen beispielsweise ein Virenfund oder eine Funktionsstörung.

- *Wichtige Ereignisse*. Ereignisse, die unbedingt beachtet werden müssen, weil sie auf Situationen bei der Programmarbeit hinweisen, die Ihre Reaktion erfordern (z.B. Ereignis wurde **abgebrochen**).

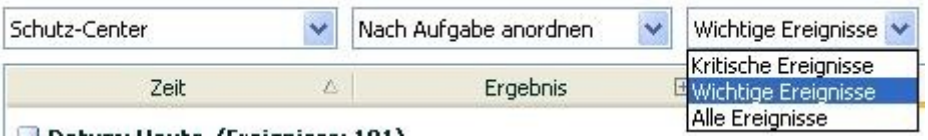

Abbildung 14: Ereignistyp wählen

Entscheiden Sie sich für den Punkt **Alle Ereignisse**, werden im Bericht alle Ereignisse angezeigt, jedoch nur dann, wenn im Abschnitt **Berichte und Speicher** im Block **Berichte** die Häkchen in den Kontrollkästchen (s. Abschnitt "Einträge über Ereignisse zum Bericht hinzufügen" auf S. 184) gesetzt sind, mit denen in den Bericht Einträge über unkritische Ereignisse sowie Ereignisse des Dateisystems und der Registrierung gemacht werden dürfen. Wenn die Kontrollkästchen nicht aktiviert sind, werden neben der Dropdown-Liste, die der Auswahl von Ereignistypen dient, ein Warnsymbol und der Link **Deaktiviert** angezeigt. Verwenden Sie diesen Link, um in das Fenster zum Anpassen von Berichten zu gehen und die entsprechenden Kontrollkästchen zu aktivieren.

➡ *Gehen Sie folgendermaßen vor, um einen Ereignistyp auszuwählen, für den ein Bericht erstellt werden soll:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Bericht**.

2. Klicken Sie im folgenden Fenster auf der Registerkarte **Bericht** auf die Schaltfläche **Vollständiger Bericht**.

3. Wählen Sie im folgenden Fenster in der Dropdown-Liste einen Ereignistyp aus. Wenn ein Bericht über alle Ereignisse erstellt werden soll, wählen Sie den Wert **Alle Ereignisse** aus.

DARSTELLUNG VON DATEN AUF DEM BILDSCHIRM

Die im Bericht enthaltenen Ereignisse werden in Tabellenform dargestellt. Sie können steuern, welche Informationen angezeigt werden sollen, indem Sie Beschränkungsbedingungen angeben. Führen Sie dazu links von der Überschrift der Tabellenspalte, für die eine Beschränkung festgelegt werden soll, einen Linksklick aus. Die Dropdown-Liste enthält die Beschränkungen, z.B. **Gestern –** für die Spalte **Zeit**, **E-Mail-Nachricht –** für die Spalte **Objekt** usw. Wählen Sie den erforderlichen Wert aus. Sie können die erforderliche Beschränkung auswählen. Die Datenanzeige erfolgt dann unter Berücksichtigung der festgelegten Beschränkung. Wenn alle Daten angezeigt werden sollen, wählen Sie in der Beschränkungsliste den Punkt **Alle** aus.

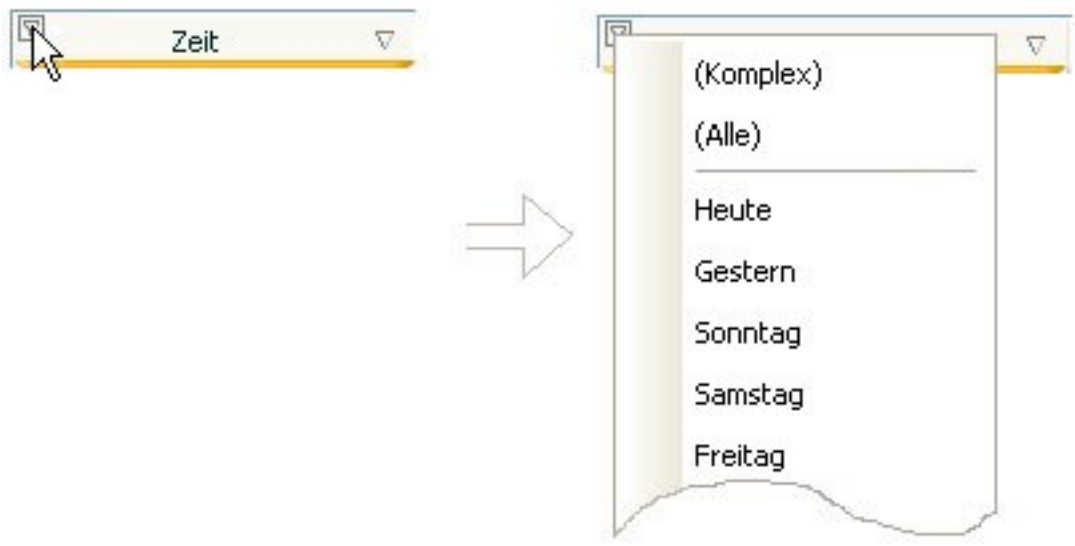

Abbildung 15: Einschränkende Bedingungen eingeben

Außerdem können Sie die komplexen Suchparameter in Form eines Intervalls angeben, innerhalb dessen der Zugriff auf die vorgefallenen Ereignisse erfolgen soll. Wählen Sie dazu in der Dropdown-Liste für Beschränkungen den Punkt **Komplex** aus. Im nächsten Fenster geben Sie den gewünschten Intervall (s. Abschnitt "Verwendung der komplexen Filterung" auf S. 204) ein.

Um die Arbeit mit der Registerkarte bequem und einfach zu gestalten, gibt es ein Kontextmenü, mit dessen Hilfe der schnelle Zugriff auf ein beliebiges Merkmal möglich ist, das die Anordnung und Auswahl von Ereignissen erlaubt.

Abbildung 16: Kontextmenü

- *Gehen Sie folgendermaßen vor, um eine Beschränkungsbedingung festzulegen:*

  1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Bericht**.

  2. Klicken Sie im folgenden Fenster auf der Registerkarte **Bericht** auf die Schaltfläche **Vollständiger Bericht**.

  3. Führen Sie dazu im folgenden Fenster links von der Überschrift der Tabellenspalte, für die eine Beschränkung festgelegt werden soll, einen Linksklick aus. Wählen Sie in der Dropdown-Liste die erforderliche Beschränkung aus. Bei Entscheidung für den Punkt **Komplex** können Sie komplexe Filterbedingungen (s. Abschnitt "Verwendung der komplexen Filterung" auf S. 204) eingeben.

- *Gehen Sie folgendermaßen vor, um die Spalten einer Tabelle auszublenden / einzublenden:*

  1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Bericht** im oberen Bereich des Fensters.

  2. Klicken Sie im folgenden Fenster auf der Registerkarte **Bericht** auf die Schaltfläche **Vollständiger Bericht**.

  3. Führen Sie im folgenden Fenster rechts von der Überschrift einer beliebigen Tabellenspalte einen Rechtsklick aus. Um bestimmte Spalten der Tabelle auszublenden, deaktivieren Sie im Kontextmenü die Kontrollkästchen der entsprechenden Bezeichnungen.

DARSTELLUNG DER STATISTIK ALS TABELLE ODER GRAFIK

Der untere Bereich des Berichtsfensters bietet eine Statistik über die Arbeit der ausgewählten Funktion oder Aufgabe von Kaspersky Internet Security. Sie können die Statistik ansehen und sie als Grafik (für Komponenten) oder in Tabellenform darstellen lassen. Die Art der Darstellung wird mit Hilfe der Schaltflächen und im oberen Bereich des Fensters gewählt. Die Statistik zeigt Informationen für den aktuellen Tag und den gesamten Zeitraum, während dem das Programm auf dem Computer arbeitet.

Gehen Sie folgendermaßen vor, um die Darstellungsweise der Statistik auszuwählen:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Bericht** im oberen Bereich des Fensters.
2. Klicken Sie im folgenden Fenster auf der Registerkarte **Bericht** auf die Schaltfläche **Vollständiger Bericht**.
3. Wählen Sie im folgenden Fenster die Programmkomponente aus, für die eine Statistik angezeigt werden soll, und verwenden Sie die Schaltflächen und im oberen Bereich des Fensters.

BERICHT IN DATEI SPEICHERN

Der Bericht kann in einer Datei gespeichert werden.

Gehen Sie folgendermaßen vor, um einen Bericht in einer Datei zu speichern:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Bericht** im oberen Bereich des Fensters.
2. Klicken Sie im folgenden Fenster auf der Registerkarte **Bericht** auf die Schaltfläche **Vollständiger Bericht**.
3. Erstellen Sie im folgenden Fenster den gewünschten Bericht und klicken Sie auf die Schaltfläche **Speichern**.
4. Geben Sie im folgenden Fenster den Ordner an, in dem die Berichtsdatei gespeichert werden soll, und nennen Sie einen Dateinamen.

VERWENDUNG DER KOMPLEXEN FILTERUNG

Das Fenster **Komplexer Filter** (s. Abbildung unten) dient dazu, die Bedingungen für die Datenfilterung zu definieren. In diesem Fenster können Sie die Intervalle für die Datensuche in einer beliebigen Spalte der Tabelle festlegen. Im Folgenden werden die Arbeitsprinzipien für dieses Fenster am Beispiel der Spalte **Zeit** beschrieben.

Der Datenzugriff mit Hilfe eines komplexen Filters basiert den Operationen Konjunktion (logisches UND) und Disjunktion (logisches ODER), mit deren Hilfe sich der Datenzugriff steuern lässt.

In den Feldern, die sich auf der rechten Seite des Fensters befinden, werden die Grenzen des Zugriffs, in diesem Fall die Zeit, angegeben. Zur Angabe der Zeit können Sie die Pfeiltasten auf der Tastatur verwenden. Auf der linken Seite**,** in der Dropdown-Liste **Bedingung,** werden die Zugriffsbedingungen für Ereignisse gewählt. **"Größer"** bedeutet beispielsweise größer als der im Feld rechts angegebene Wert.

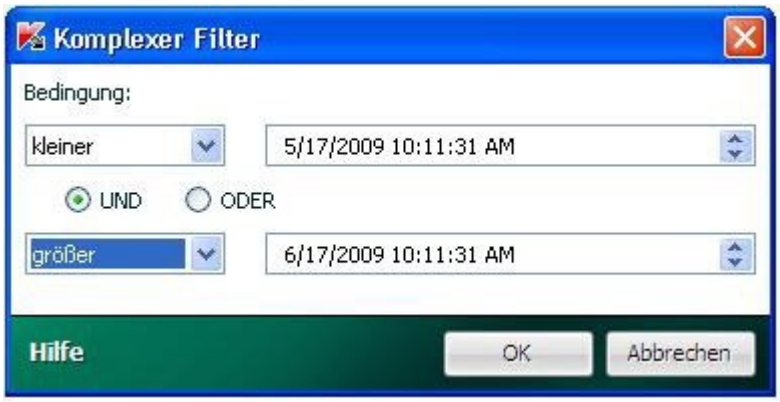

Abbildung 17: Komplexe Filterbedingungen eingeben

Wenn Sie möchten, dass er Datenzugriff beide festgelegte Bedingungen erfüllt, wählen Sie **UND** aus. Ist eine Bedienung ausreichend, dann wählen Sie **ODER** aus.

Für bestimmte Spalten gilt kein Zahlen- oder Zeitwert als Grenze des Suchintervalls, sondern ein Wort (z.B. das Untersuchungsergebnis **OK** für die Spalte **Ergebnis**). In diesem Fall wird das als Grenze angegebene Wort dem Alphabet nach mit den anderen Wortwerten für die gewählte Spalte verglichen.

Gehen Sie folgendermaßen vor, um komplexe Filterbedingungen festzulegen::

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Bericht** im oberen Bereich des Fensters.

2. Klicken Sie im folgenden Fenster auf der Registerkarte **Bericht** auf die Schaltfläche **Vollständiger Bericht**.

3. Führen Sie im folgenden Fenster links von der Überschrift der Tabellenspalte, für die komplexe Filterbedingungen festgelegt werden sollen, einen Linksklick aus. Wählen Sie im Kontextmenü den Punkt **Komplex** aus. Außerdem können Sie auf den Punkt **Filter** im Kontextmenü (s. Abschnitt "Darstellung von Daten auf dem Bildschirm" auf S. 202) gehen, der mit einem Klick auf die rechte Maustaste auf die gewünschte Tabellenspalte verfügbar wird.

4. Legen Sie im folgenden Fenster **Komplexer Filter** die erforderlichen Filterbedingungen fest.

SUCHE NACH EREIGNISSEN

Dieses Fenster (siehe Abbildung unten) dient der Suche nach Ereignissen, die im System aufgetreten und von Kaspersky Internet Security verarbeitet wurden.

Im Folgenden werden die Prinzipien der Arbeit in diesem Fenster beschrieben:

- Das Feld **Zeile** dient der Eingabe von Schlüsselwörtern (z.B. Explorer). Klicken Sie auf die Schaltfläche **Weitersuchen**, um die Suche zu starten. Die Suche nach Daten kann eine gewisse Zeit beanspruchen. Nach Abschluss der Suche werden die Ereignisse angezeigt, die dem angegebenen Schlüsselwort entsprechen. Durch Klick auf die Schaltfläche **Alle markieren** werden alle gefundenen Daten, die dem festgelegten Schlüsselwort entsprechen, markiert.

- Das Feld **Spalte** erlaubt die Auswahl der Tabellenspalte, nach der die Suche nach dem Schlüsselwort ausgeführt wird. Eine solche Auswahl erlaubt es, die Suchdauer zu verkürzen (falls nicht der Wert **Alle** gewählt wurde).

Abbildung 18: Suche nach Ereignissen

Wenn bei der Suche die Groß- und Kleinschreibung für das Schlüsselwort berücksichtigt werden soll, aktivieren Sie das Kontrollkästchen ☑ **Groß- und Kleinschreibung**. Das Kontrollkästchen ☑ **Nur ganze Wörter** erlaubt es, die Suche nach dem Schlüsselwort auf das Vorkommen ganzer Wörter zu beschränken.

Gehen Sie folgendermaßen vor, um die Ereignissuche zu verwenden:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Bericht** im oberen Bereich des Fensters.

2. Klicken Sie im folgenden Fenster auf der Registerkarte **Bericht** auf die Schaltfläche **Vollständiger Bericht**.

3. Führen Sie im folgenden Fenster rechts von der Überschrift einer beliebigen Tabellenspalte einen Rechtsklick aus. Wählen sie im Kontextmenü den Punkt **Suche** aus.

4. Legen Sie im folgenden Fenster **Suche** die Suchkriterien fest.

MELDUNGEN

Beim Auftreten bestimmter Ereignisse während der Arbeit von Kaspersky Internet Security werden auf dem Bildschirm spezielle Meldungen angezeigt. In Abhängigkeit davon, welche Relevanz das Ereignis für die Computersicherheit besitzt, sind folgende Arten von Meldungen möglich:

- **Alarm**. Ein Ereignis mit kritischer Priorität ist eingetreten. Beispiele: "Ein schädliches Objekt wurde gefunden" oder "Im System wurde eine gefährliche Aktivität erkannt". Die sofortige Entscheidung über das weitere Vorgehen ist erforderlich. Ein Fenster mit Meldungen dieses Typs ist rot.

- **Warnung**. Ein potentiell gefährliches Ereignis hat sich ereignet. Beispiele: "Ein möglicherweise infiziertes Objekt wurde gefunden" oder "Im System wurde verdächtige Aktivität erkannt". Sie müssen entscheiden, inwieweit diese Aktion nach Ihrem Ermessen gefährlich ist. Ein Fenster mit Meldungen dieses Typs ist gelb.

- **Info**. Diese Meldung informiert über ein Ereignis, das keine vorrangige Priorität besitzt. Ein Fenster mit Meldungen dieses Typs ist grün.

Das Meldungsfenster besteht aus vier Elementen:

1. *Fenstertitel*. Die Überschrift der Meldung enthält eine kurze Beschreibung des Ereignisses, z.B. Anfrage auf Rechte, verdächtige Aktivität, neues Netzwerk, Alarm, Virus.

2. *Ereignisbeschreibung*. Im Block Ereignisbeschreibung werden ausführliche Informationen über den Grund für die Meldung genannt: Name des Programms, das das Ereignis hervorgerufen hat; Name der gefundenen Bedrohung; Parameter der gefundenen Netzwerkverbindung u.a.

3. *Bereich zur Aktionsauswahl*. In diesem Block können Sie eine der für dieses Ereignis möglichen Aktionen auswählen. Die zur Auswahl angebotenen Aktionen sind vom Ereignistyp abhängig, beispielsweise: **Desinfizieren**, **Löschen**, **Überspringen –** bei einem Virenfund, **Erlauben**, **Verbieten –** wenn eine Anwendung Rechte zur Ausführung potentiell gefährlicher Aktionen fordert. Die von den Kaspersky-Lab-Spezialisten empfohlene Aktion ist durch fette Schrift hervorgehoben.

   Bei Auswahl der Aktion **Erlauben** oder **Verbieten** wird ein Fenster geöffnet, in dem ein *Modus für die Anwendung der Aktion* ausgewählt werden kann. Für die Aktion **Erlauben** können Sie einen der folgenden Modi auswählen:

   - **Immer erlauben**. Wählen Sie diese Variante aus, um eine erkannte Programmaktivität zu erlauben und gleichzeitig die Regel für den Zugriff des Programms auf Systemressourcen entsprechend zu ändern.

   - **Jetzt erlauben**. Aktivieren Sie dieses Kontrollkästchen, damit die gewählte Aktion auf alle ähnlichen Ereignisse, die während der Programmsitzung gefunden werden, angewandt wird. Als Programmsitzung gilt die Arbeitszeit ab dem Programmstart bis zum Beenden oder Neustart des Programms.

   - **Vertrauenswürdig machen**. Wählen Sie diese Variante aus, um das Programm in die Gruppe **Vertrauenswürdig** zu verschieben.

   Für die Aktion **Verbieten** können Sie einen der folgenden Modi auswählen:

   - **Immer verbieten**. Wählen Sie diese Variante aus, um eine erkannte Programmaktivität zu verbieten und gleichzeitig die Regel für den Zugriff des Programms auf Systemressourcen entsprechend zu ändern.

   - **Jetzt verbieten**. Aktivieren Sie dieses Kontrollkästchen, damit die gewählte Aktion auf alle ähnlichen Ereignisse, die während der Programmsitzung gefunden werden, angewandt wird. Als Programmsitzung gilt die Arbeitszeit ab dem Programmstart bis zum Beenden oder Neustart des Programms.

   - **Beenden**. Wählen Sie diese Variante aus, um die Arbeit des Programms abzubrechen.

4. *Bereich zur Auswahl einer zusätzlichen Aktion*. In diesem Block kann eine zusätzliche Aktion ausgewählt werden:

- **Zu Ausnahmen hinzufügen**. Wenn Sie überzeugt sind, dass das gefundene Objekt ungefährlich ist, können Sie es der vertrauenswürdigen Zone hinzufügen, um zu verhindern, dass das Programm bei der Arbeit mit diesem Objekt erneut anspricht.

- **Auf alle Objekte anwenden**. Aktivieren Sie dieses Kontrollkästchen, damit die gewählte Aktion in ähnlichen Situationen auf alle Objekte mit dem gleichen Status angewandt wird.

IN DIESEM ABSCHNITT

Verdächtiges Objekt wurde gefunden....208

Desinfektion des Objekts ist nicht möglich....209

Spezielle Desinfektionsprozedur ist erforderlich....209

Gefährliches Objekt wurde im Datenstrom gefunden....210

Verdächtiges Objekt wurde gefunden....210

Gefährliche Aktivität im System wurde erkannt....211

Versteckter Prozess wurde gefunden....212

Versuch zum Zugriff auf die Systemregistrierung wurde erkannt....212

Netzwerkaktivität eines Programms wurde erkannt....213

Neues Netzwerk wurde gefunden....214

Phishing-Angriff wurde erkannt....214

Verdächtiger Link wurde gefunden....214

Ein inkorrektes Zertifikat wurde gefunden....215

VERDÄCHTIGES OBJEKT WURDE GEFUNDEN

Wenn von Datei-Anti-Virus, Mail-Anti-Virus oder von einer Untersuchungsaufgabe ein schädliches Objekt gefunden wird, erscheint eine spezielle Meldung auf dem Bildschirm.

Sie enthält:

- Art der Bedrohung (beispielsweise *Virus*, *trojanisches Programm*) und Name des schädlichen Objekts, der seiner Bezeichnung in der Viren-Enzyklopädie von Kaspersky Lab entspricht. Der Name des schädlichen Objekts besitzt die Form eines Links zu der Ressource http://www.viruslist.com/de, auf der Sie ausführliche Informationen darüber erhalten können, welche Art von Bedrohung auf Ihrem Computer gefunden wurde.

- Vollständiger Name und Pfad des schädlichen Objekts.

Ihnen wird angeboten, eine der folgenden Aktionen für das Objekt auszuwählen:

- **Desinfizieren** – Es wird versucht, das schädliche Objekt zu desinfizieren. Vor der Desinfektion wird eine Sicherungskopie des Objekts angelegt, um bei Bedarf das Objekt oder ein Infektionsbild wiederherstellen zu können.

- **Löschen** – Das schädliche Objekt löschen. Vor dem Löschen wird eine Sicherungskopie des Objekts angelegt, um bei Bedarf das Objekt oder ein Infektionsbild wiederherstellen zu können.

- **Überspringen** - Der Zugriff auf das Objekt wird gesperrt. Keine Aktion mit dem Objekt vornehmen, sondern nur Informationen darüber im Bericht aufzeichnen.

  Sie können später aus dem Berichtsfenster zur Verarbeitung von übersprungenen schädlichen Objekten zurückkehren (für Objekte, die in E-Mails gefunden wurden, steht die Option zur aufgeschobenen Verarbeitung nicht zur Verfügung).

Damit die ausgewählte Aktion auf alle Objekte mit dem gleichen Status angewendet wird, die während der laufenden Sitzung der Schutzkomponente oder Aufgabe gefunden werden, aktivieren Sie das Kontrollkästchen ☑ **In allen ähnlichen Fällen anwenden**. Als laufende Sitzung gilt die Arbeitszeit einer Komponente ab dem Zeitpunkt ihres Starts bis zum Moment des Abschaltens oder Neustarts des Programms, sowie die Ausführungszeit einer Untersuchungsaufgabe ab dem Start bis zum Abschluss.

DESINFEKTION DES OBJEKTS IST NICHT MÖGLICH

In bestimmten Fällen ist die Desinfektion eines schädlichen Objekts nicht möglich. So kann eine Datei beispielsweise so stark beschädigt sein, dass es nicht möglich ist, den schädlichen Code daraus zu löschen und sie vollständig wiederherzustellen. Außerdem ist die Desinfektionsprozedur bei einigen Arten von schädlichen Objekten wie z.B. Trojaner-Programme nicht anwendbar.

In solchen Fällen erscheint auf dem Bildschirm eine spezielle Meldung, die folgende Informationen enthält:

- Art der Bedrohung (beispielsweise *Virus*, *trojanisches Programm*) und Name des schädlichen Objekts, der seiner Bezeichnung in der Viren-Enzyklopädie von Kaspersky Lab entspricht. Der Name des schädlichen Objekts besitzt die Form eines Links zu der Ressource http://www.viruslist.com/de, auf der Sie ausführliche Informationen darüber erhalten können, welche Art von Bedrohung auf Ihrem Computer gefunden wurde.

- Vollständiger Name und Pfad des schädlichen Objekts.

Ihnen wird angeboten, eine der folgenden Aktionen für das Objekt auszuwählen:

- **Löschen** – Das schädliche Objekt löschen. Vor dem Löschen wird eine Sicherungskopie des Objekts angelegt, um bei Bedarf das Objekt oder ein Infektionsbild wiederherstellen zu können.

- **Überspringen** - Der Zugriff auf das Objekt wird gesperrt. Keine Aktion mit dem Objekt vornehmen, sondern nur Informationen darüber im Bericht aufzeichnen.

  Sie können später aus dem Berichtsfenster zur Verarbeitung von übersprungenen schädlichen Objekten zurückkehren (für Objekte, die in E-Mails gefunden wurden, steht die Option zur aufgeschobenen Verarbeitung nicht zur Verfügung).

Damit die ausgewählte Aktion auf alle Objekte mit dem gleichen Status angewendet wird, die während der laufenden Sitzung der Schutzkomponente oder Aufgabe gefunden werden, aktivieren Sie das Kontrollkästchen ☑ **In allen ähnlichen Fällen anwenden**. Als laufende Sitzung gelten die Arbeitszeit einer Komponente ab dem Zeitpunkt ihres Starts bis zum Moment des Ausschaltens oder Neustarts des Programms, sowie die Ausführungszeit einer Untersuchungsaufgabe ab dem Start bis zum Abschluss.

SPEZIELLE DESINFEKTIONSPROZEDUR IST ERFORDERLICH

Beim Fund einer Bedrohung, die gerade im System aktiv ist (beispielsweise ein schädlicher Prozess im Arbeitsspeicher oder in den Autostart-Objekten), erscheint auf dem Bildschirm eine Eingabeaufforderung zum Durchführen einer speziell dafür vorgesehenen erweiterten Desinfektionsprozedur.

Die Spezialisten von Kaspersky Lab empfehlen ausdrücklich, in solchen Fällen die erweiterte Desinfektionsprozedur durchzuführen. Klicken Sie dazu auf die Schaltfläche **OK**. Beachten Sie aber, dass zum Abschluss des Vorgangs der Computer neu gestartet wird. Deshalb sollten die aktuellen Arbeitsergebnisse gespeichert und alle Anwendungen geschlossen werden, bevor der Vorgang ausgeführt wird.

Während der Desinfektionsvorgang ausgeführt wird, sind der Start von Mailprogrammen und das Ändern der Registrierung des Betriebssystems verboten. Nach dem Neustart des Computers wird empfohlen, die vollständige Virenuntersuchung zu starten.

GEFÄHRLICHES OBJEKT WURDE IM DATENSTROM GEFUNDEN

Wenn Web-Anti-Virus im Datenstrom ein gefährliches Objekt findet, erscheint eine spezielle Meldung auf dem Bildschirm.

Die Meldung enthält:

- Art der Bedrohung (beispielsweise *Virusmodifikation*) und Name des gefährlichen Objekts, der seiner Bezeichnung in der Viren-Enzyklopädie von Kaspersky Lab entspricht. Der Name des Objekts besitzt die Form eines Links zu der Webseite http://www.viruslist.com/de, auf der Sie ausführliche Informationen darüber erhalten können, welche Art von Bedrohung auf Ihrem Computer gefunden wurde.

- Vollständiger Name des gefährlichen Objekts und Pfad der Webseite.

Ihnen wird angeboten, eine der folgenden Aktionen für das Objekt auszuwählen:

- **Erlauben** - Download des Objekts fortsetzen.

- **Verbieten** – Download des Objekts von der Webseite blockieren.

Damit die ausgewählte Aktion auf alle Objekte mit dem gleichen Status angewendet wird, die während der laufenden Sitzung der Schutzkomponente oder Aufgabe gefunden werden, aktivieren Sie das Kontrollkästchen ☑ **In allen ähnlichen Fällen anwenden**. Als laufende Sitzung gilt die Arbeitszeit einer Komponente ab dem Zeitpunkt ihres Starts bis zum Moment des Abschaltens oder Neustarts des Programms, sowie die Ausführungszeit einer Untersuchungsaufgabe ab dem Start bis zum Abschluss.

VERDÄCHTIGES OBJEKT WURDE GEFUNDEN

Wenn von Datei-Anti-Virus, Mail-Anti-Virus oder von einer Untersuchungsaufgabe ein Objekt gefunden wird, das den Code eines unbekannten Virus oder den modifizierten Code eines bekannten Virus enthält, erscheint eine spezielle Meldung auf dem Bildschirm.

Sie enthält:

- Art der Bedrohung (beispielsweise *Virus*, *trojanisches Programm*) und Name des Objekts, der seiner Bezeichnung in der Viren-Enzyklopädie von Kaspersky Lab entspricht. Der Name des schädlichen Objekts besitzt die Form eines Links zu der Ressource http://www.viruslist.com/de, auf der Sie ausführliche Informationen darüber erhalten können, welche Art von Bedrohung auf Ihrem Computer gefunden wurde.

- Vollständiger Name und Pfad des Objekts.

Ihnen wird angeboten, eine der folgenden Aktionen für das Objekt auszuwählen:

- **Quarantäne** - Das Objekt wird in die Quarantäne verschoben. Ein Objekt unter Quarantäne zu stellen, bedeutet, es wird nicht kopiert, sondern verschoben: Das Objekt wird am ursprünglichen Speicherort oder aus einer E-Mail-Nachricht gelöscht und im Quarantäneordner gespeichert. Die unter Quarantäne stehenden Dateien werden in einem speziellen Format gespeichert und stellen keine Gefahr dar.

  Bei späteren Untersuchungen der Quarantäne mit aktualisierten Bedrohungssignaturen kann sich der Status eines Objekts ändern. Das Objekt kann beispielsweise als infiziert erkannt und mit Hilfe aktualisierter Datenbanken verarbeitet werden, oder es erhält den Status *virenfrei* und kann dann wiederhergestellt werden.

  Wenn sich eine Datei, die manuell in die Quarantäne verschoben wurde, bei einer späteren Untersuchung als

virenfrei erweist, ändert sich ihr Status nicht gleich nach der Untersuchung in *ok*. Der Status ändert sich nur dann sofort, wenn die Untersuchung mindestens drei Tage, nachdem die Datei unter Quarantäne gestellt wurde, stattfindet.

- **Löschen** – Das Objekt löschen. Vor dem Löschen wird eine Sicherungskopie des Objekts angelegt, um bei Bedarf das Objekt oder ein Infektionsbild wiederherstellen zu können.
- **Überspringen** - Der Zugriff auf das Objekt wird gesperrt. Keine Aktion mit dem Objekt vornehmen, sondern nur Informationen darüber im Bericht aufzeichnen.

  Sie können später aus dem Berichtsfenster zur Verarbeitung von übersprungenen schädlichen Objekten zurückkehren (für Objekte, die in E-Mails gefunden wurden, steht die Option zur aufgeschobenen Verarbeitung nicht zur Verfügung).

Damit die ausgewählte Aktion auf alle Objekte mit dem gleichen Status angewendet wird, die während der laufenden Sitzung der Schutzkomponente oder Aufgabe gefunden werden, aktivieren Sie das Kontrollkästchen **In allen ähnlichen Fällen anwenden**. Als laufende Sitzung gilt die Arbeitszeit einer Komponente ab dem Zeitpunkt ihres Starts bis zum Moment des Abschaltens oder Neustarts des Programms, sowie die Ausführungszeit einer Untersuchungsaufgabe ab dem Start bis zum Abschluss.

Wenn Sie überzeugt sind, dass das gefundene Objekt ungefährlich ist, können Sie es der vertrauenswürdigen Zone hinzufügen, um zu verhindern, dass das Programm bei der Arbeit mit diesem Objekt erneut anspricht.

GEFÄHRLICHE AKTIVITÄT IM SYSTEM WURDE ERKANNT

Wenn der Proaktive Schutz die gefährliche Aktivität einer bestimmten Anwendung im System erkennt, wird auf dem Bildschirm eine spezielle Meldung angezeigt, die folgende Informationen enthält:

- Name der Bedrohung, der ihrer Bezeichnung in der Viren-Enzyklopädie von Kaspersky Lab entspricht. Der Name der Bedrohung besitzt die Form eines Links zu der Ressource http://www.viruslist.com/de, auf der Sie ausführliche Informationen darüber erhalten können, welche Art von Bedrohung auf Ihrem Computer gefunden wurde.
- Vollständiger Dateiname und Pfad des Prozesses, der die gefährliche Aktivität initiierte.
- Auswahl möglicher Aktionen:
  - **Quarantäne** - Prozess beenden und die ausführbare Datei des Prozesses in die Quarantäne verschieben. Wenn das Objekt in der Quarantäne gespeichert wird, wird es verschoben, nicht kopiert: Die unter Quarantäne stehenden Dateien werden in einem speziellen Format gespeichert und stellen keine Gefahr dar.

    Bei späteren Untersuchungen der Quarantäne mit aktualisierten Bedrohungssignaturen kann sich der Status eines Objekts ändern. Das Objekt kann beispielsweise als infiziert erkannt und mit Hilfe aktualisierter Datenbanken verarbeitet werden, oder es erhält den Status *virenfrei* und kann dann wiederhergestellt werden.

    Wenn sich eine Datei, die manuell in die Quarantäne verschoben wurde, bei einer späteren Untersuchung als virenfrei erweist, ändert sich ihr Status nicht gleich nach der Untersuchung in *ok*. Der Status ändert sich nur dann sofort, wenn die Untersuchung mindestens drei Tage, nachdem die Datei unter Quarantäne gestellt wurde, stattfindet.

  - **Beenden** - Prozess beenden.
  - **Erlauben** - Das Ausführen des Prozesses erlauben.

Damit die ausgewählte Aktion auf alle Objekte mit dem gleichen Status angewendet wird, die während der laufenden Sitzung der Schutzkomponente oder Aufgabe gefunden werden, aktivieren Sie das Kontrollkästchen **In allen ähnlichen Fällen anwenden**. Als laufende Sitzung gilt die Arbeitszeit einer Komponente ab dem Zeitpunkt ihres Starts

bis zum Moment des Abschaltens oder Neustarts des Programms, sowie die Ausführungszeit einer Untersuchungsaufgabe ab dem Start bis zum Abschluss.

Wenn Sie überzeugt sind, dass das gefundene Programm ungefährlich ist, können Sie es der vertrauenswürdigen Zone hinzufügen, um zu verhindern, dass Kaspersky Internet Security erneut anspricht, wenn er das Programm findet.

VERSTECKTER PROZESS WURDE GEFUNDEN

Wenn der Proaktive Schutz einen versteckten Prozess im System findet, erscheint auf dem Bildschirm eine spezielle Meldung, die folgende Informationen enthält:

- Name der Bedrohung, der ihrer Bezeichnung in der Viren-Enzyklopädie von Kaspersky Lab entspricht. Der Name der Bedrohung besitzt die Form eines Links zu der Ressource http://www.viruslist.com/de, auf der Sie ausführliche Informationen darüber erhalten können, welche Art von Bedrohung auf Ihrem Computer gefunden wurde.
- Vollständiger Dateiname und Pfad des versteckten Prozesses.
- Auswahl möglicher Aktionen:
  - **Quarantäne** - Die ausführbare Prozessdatei wird in die Quarantäne verschoben. Wenn das Objekt in der Quarantäne gespeichert wird, wird es verschoben, nicht kopiert: Die unter Quarantäne stehenden Dateien werden in einem speziellen Format gespeichert und stellen keine Gefahr dar.

    Bei späteren Untersuchungen der Quarantäne mit aktualisierten Bedrohungssignaturen kann sich der Status eines Objekts ändern. Das Objekt kann beispielsweise als infiziert erkannt und mit Hilfe aktualisierter Datenbanken verarbeitet werden, oder es erhält den Status *virenfrei* und kann dann wiederhergestellt werden.

    Wenn sich eine Datei, die manuell in die Quarantäne verschoben wurde, bei einer späteren Untersuchung als virenfrei erweist, ändert sich ihr Status nicht gleich nach der Untersuchung in *ok*. Der Status ändert sich nur dann sofort, wenn die Untersuchung mindestens drei Tage, nachdem die Datei unter Quarantäne gestellt wurde, stattfindet.
  - **Beenden** - Prozess beenden.
  - **Erlauben** - Das Ausführen des Prozesses erlauben.

Damit die ausgewählte Aktion auf alle Objekte mit dem gleichen Status angewendet wird, die während der laufenden Sitzung der Schutzkomponente oder Aufgabe gefunden werden, aktivieren Sie das Kontrollkästchen **In allen ähnlichen Fällen anwenden**. Als laufende Sitzung gilt die Arbeitszeit einer Komponente ab dem Zeitpunkt ihres Starts bis zum Moment des Abschaltens oder Neustarts des Programms, sowie die Ausführungszeit einer Untersuchungsaufgabe ab dem Start bis zum Abschluss.

Wenn Sie überzeugt sind, dass das gefundene Programm ungefährlich ist, können Sie es der vertrauenswürdigen Zone hinzufügen, um zu verhindern, dass Kaspersky Internet Security erneut anspricht, wenn er das Programm findet.

VERSUCH ZUM ZUGRIFF AUF DIE SYSTEMREGISTRIERUNG WURDE ERKANNT

Wenn der Proaktive Schutz erkennt, dass versucht wird, auf Schlüssel der Systemregistrierung zuzugreifen, erscheint auf dem Bildschirm eine spezielle Meldung, die folgende Informationen enthält:

- Registrierungsschlüssel, auf den der Zugriffsversuch erfolgte.
- Vollständiger Dateiname und Pfad des Prozesses, der versuchte auf Registrierungsschlüssel zuzugreifen.

- Auswahl möglicher Aktionen:
  - **Erlauben** - Das Ausführen der gefährlichen Aktion einmal erlauben.
  - **Verbieten** - Das Ausführen der gefährlichen Aktion einmal verbieten.

Damit die von Ihnen ausgewählte Aktion jedes Mal automatisch ausgeführt wird, wenn diese Aktivität auf Ihrem Computer initiiert wird, aktivieren Sie das Kontrollkästchen ☑ **Regel erstellen**.

Wenn Sie überzeugt sind, dass jede Aktivität der Anwendung, die den Zugriff auf die Systemregistrierungsschlüssel initiierte, ungefährlich ist, fügen Sie diese Anwendung der Liste der vertrauenswürdigen Anwendungen hinzu.

NETZWERKAKTIVITÄT EINES PROGRAMMS WURDE ERKANNT

Wenn die Netzwerkaktivität eines Programms erkannt wird, erscheint auf dem Bildschirm eine Meldung (standardmäßig für Programme der Gruppen (s. Abschnitt "Programmgruppen" auf S. 76) **Schwach beschränkt** oder **Stark beschränkt**).

Es wird eine Meldung angezeigt, wenn Kaspersky Internet Security im interaktiven Modus (s. Abschnitt "Interaktiven Schutzmodus verwenden" auf S. 160), arbeitet und für das Programm, dessen Netzwerkaktivität erkannt wurde, keine Paketregel (s. S. 92) erstellt wurde.

Die Meldung enthält:

- *Beschreibung der Aktivität* – Name der Anwendung und kurze Charakteristik der Verbindung, die sie initiiert hat. In der Regel werden folgende Angaben genannt: Verbindungstyp, lokaler Port, von dem aus die Verbindung initiiert wurde, Remoteport und Adresse, mit der die Verbindung ausgeführt wird.
- *Startfolge eines Programms*.
- *Aktion* – Operationsfolge, die Kaspersky Internet Security im Hinblick auf die gefundene Netzwerkaktivität ausführen soll.

Ihnen wird angeboten, eine der folgenden Aktionen auszuwählen:

- **Erlauben**.
- **Verbieten**.
- **Regel erstellen**. Bei Auswahl dieser Variante wird der *Assistent für neue Regeln* gestartet (s. S. 94), der Sie dabei unterstützt, eine Regel für die Netzwerkaktivität des Programms zu erstellen.

Sie können:

- Aktion ein Mal ausführen. Wählen Sie dazu die Variante **Erlauben** oder **Verbieten** aus.
- Aktion speichern für die Sitzung des Programms, die eine Netzwerkaktivität gezeigt hat. Wählen Sie dazu die Variante **Erlauben** oder **Verbieten** aus und aktivieren Sie das Kontrollkästchen ☑ **Speichern für diese Programmsitzung**.
- für das Programm ausgewählte Aktion für immer speichern. Wählen Sie dazu die Variante **Erlauben** oder **Verbieten** und aktivieren Sie das Kontrollkästchen ☑ **Speichern für immer**.
- Regel für die Netzwerkaktivität des Programms erstellen. Wählen Sie dazu die Variante **Regel erstellen**.

NEUES NETZWERK WURDE GEFUNDEN

Bei jeder Verbindung des Computers mit einer neuen Zone (Netzwerk) erscheint auf dem Bildschirm eine spezielle Meldung.

Der obere Bereich der Meldung enthält eine kurze Beschreibung des Netzwerks mit Angabe der IP-Adresse und Subnetzmaske.

Im unteren Teil können Sie einen Status für die gefundene Zone festlegen, auf dessen Grundlage entschieden wird, welche Art von Netzwerkaktivität erlaubt wird:

- **Öffentliches Netzwerk (Externen Zugriff auf den Computer verbieten)**. Netzwerk mit hoher Risikostufe. Bei der Arbeit in dieser Zone ist der Computer allen möglichen Typen von Bedrohungen ausgesetzt. Dieser Status wird auch für Netzwerke empfohlen, die nicht durch Antiviren-Programme, Firewalls, Filter usw. geschützt werden. Die Auswahl dieses Status gewährleistet dem Computer bei der Arbeit in dieser Zone maximale Sicherheit.

- **Lokales Netzwerk (Zugriff auf Dateien und Drucker erlauben)**. Es wird empfohlen, diesen Status für Zonen mit mittlerer Risikostufe anzuwenden (beispielsweise für interne Firmennetzwerk).

- **Vertrauenswürdiges Netzwerk (Jede Netzwerkaktivität erlauben)**. Es wird empfohlen, diesen Status nur für absolut sichere Zonen zu verwenden, in denen dem Computer keine Angriffe und Versuche zum unerlaubten Datenzugriff drohen.

PHISHING-ANGRIFF WURDE ERKANNT

Wenn Kaspersky Internet Security einen Versuch zum Öffnen einer Phishing-Seite entdeckt, erscheint auf dem Bildschirm eine spezielle Meldung.

Die Meldung enthält folgende Informationen:

- Name der Bedrohung – *Phishing-Angriff*. Der Name besitzt die Form eines Links zur Viren-Enzyklopädie von Kaspersky Lab, wo die Bedrohung ausführlich beschrieben wird.

- Web-Adresse der Phishing-Seite im Internet.

- Auswahl möglicher Aktionen:

  - **Erlauben** – Download der Phishing-Seite fortsetzen.

  - **Verbieten** – Download der Phishing-Seite blockieren.

Damit die ausgewählte Aktion auf alle Objekte mit dem gleichen Status angewendet wird, die während der laufenden Sitzung der Schutzkomponente oder Aufgabe gefunden werden, aktivieren Sie das Kontrollkästchen ☑ **In allen ähnlichen Fällen anwenden**. Als laufende Sitzung gilt die Arbeitszeit einer Komponente ab dem Zeitpunkt ihres Starts bis zum Moment des Abschaltens oder Neustarts des Programms, sowie die Ausführungszeit einer Untersuchungsaufgabe ab dem Start bis zum Abschluss.

VERDÄCHTIGER LINK WURDE GEFUNDEN

Wenn Kaspersky Internet Security erkennt, dass versucht wird, eine Webseite zu öffnen, deren Adresse auf der Liste der verdächtigen Webadressen steht, erscheint auf dem Bildschirm eine Meldung.

Die Meldung enthält folgende Informationen:

- Webadresse der Seite im Internet.

- Auswahl möglicher Aktionen:

- **Erlauben** – Download der Webseite fortsetzen.
- **Verbieten** – Download der Webseite blockieren.

Damit die ausgewählte Aktion auf alle Objekte mit dem gleichen Status angewendet wird, die während der laufenden Sitzung der Schutzkomponente oder Aufgabe gefunden werden, aktivieren Sie das Kontrollkästchen ☑ **In allen ähnlichen Fällen anwenden**. Als laufende Sitzung gilt die Arbeitszeit einer Komponente ab dem Zeitpunkt ihres Starts bis zum Moment des Abschaltens oder Neustarts des Programms, sowie die Ausführungszeit einer Untersuchungsaufgabe ab dem Start bis zum Abschluss.

EIN INKORREKTES ZERTIFIKAT WURDE GEFUNDEN

Die Zuverlässigkeit einer SSL-Verbindung wird mit Hilfe des installierten Zertifikats geprüft. Wenn beim Verbindungsversuch mit einem Server ein inkorrektes Zertifikat verwendet wird (z.B. wenn es von einem Angreifer ausgetauscht wurde), erscheint auf dem Bildschirm eine entsprechende Meldung.

Die Meldung informiert über mögliche Fehlerursachen, Remoteport und Remoteadresse. Sie werden aufgefordert zu entscheiden, ob unter Verwendung des inkorrekten Zertifikats eine Verbindung hergestellt werden soll:

- **Zertifikat akzeptieren** – Verbindung mit der Webseite fortsetzen.
- **Zertifikat ablehnen** – Verbindung mit der Webseite trennen.
- **Zertifikat anzeigen** – Informationen über das Zertifikat anzeigen.

EINSTELLUNGEN VON KASPERSKY INTERNET SECURITY AUF KORREKTHEIT PRÜFEN

Nach der Installation und Konfiguration von Kaspersky Internet Security können Sie mit Hilfe eines "Testvirus" und dessen Modifikationen prüfen, ob die Einstellungen korrekt sind. Die Prüfung muss für jede Schutzkomponente und für jedes Protokoll einzeln ausgeführt werden.

IN DIESEM ABSCHNITT

EICAR-"Testvirus" und seine Modifikationen 216

Testen des Schutzes für HTTP-Datenverkehr 218

Schutz für den SMTP-Datenverkehr testen 218

Überprüfung der Einstellungen von Datei-Anti-Virus 218

Überprüfung der Einstellungen für eine Aufgabe zur Virensuche 219

Überprüfung der Einstellungen für den Schutz vor unerwünschten E-Mails 219

EICAR-"TESTVIRUS" UND SEINE MODIFIKATIONEN

Dieser "Testvirus" wurde vom Institut eicar (The European Institute for Computer Antivirus Research) speziell zum Überprüfen der Arbeit von Antiviren-Produkten entwickelt.

Der "Testvirus" IST KEIN VIRUS und enthält keinen Programmcode, der Ihren Rechner beschädigen könnte. Trotzdem wird er von den meisten Antiviren-Softwareprodukten als Virus identifiziert.

Verwenden Sie nie echte Viren, um die Funktionsfähigkeit eines Antiviren-Produkts zu testen!

Der "Testvirus" kann von der offiziellen Internetseite des **EICAR**-Instituts heruntergeladen werden: http://www.eicar.org/anti_virus_test_file.htm.

Bevor der "Testvirus" heruntergeladen wird, muss der Antiviren-Schutz deaktiviert werden, weil die Datei *anti_virus_test_file.htm* andernfalls als infiziertes, mit dem HTTP-Protokoll übertragenes Objekt identifiziert und entsprechend behandelt wird. Vergessen Sie nicht, den Antiviren-Schutz sofort nach dem Download des "Testvirus" wieder zu aktivieren.

Die von der Webseite des **EICAR**-Instituts heruntergeladene Datei wird vom Programm als infiziertes Objekt identifiziert, das einen Virus enthält, **der nicht desinfiziert werden kann**, und führt die für diesen Objekttyp festgelegte Aktion aus.

Um die Funktion des Programms zu prüfen, können Sie auch Modifikationen des standardmäßigen "Testvirus" verwenden. Dazu wird der Inhalt des standardmäßigen "Testvirus" durch das Hinzufügen eines bestimmten Präfixes geändert (siehe Tabelle unten). **Zum Erstellen von Modifikationen des "Testvirus" eignet sich ein beliebiger Text-Editor oder Hypertext-Editor wie beispielsweise** Microsoft Editor, UltraEdit32, usw.

Die Prüfung der korrekten Funktion des Antiviren-Programms mit Hilfe eines modifizierten EICAR-"Testvirus" ist nur dann möglich, wenn die installierten Antiviren-Datenbanken nicht vor dem 24.10.2003 erschienen sind (kumulatives Update - Oktober 2003).

Die erste Spalte der Tabelle enthält Präfixe, die dem standardmäßigen "Testvirus" am Zeilenanfang hinzugefügt werden können. Die zweite Spalte zeigt die möglichen Werte für den Status, der einem Objekt aufgrund der Untersuchungsergebnisse von Anti-Virus zugewiesen werden kann. Die dritte Spalte bietet Informationen darüber, wie Objekte mit dem betreffenden Status vom Programm bearbeitet werden. Beachten Sie, dass die Aktionen für Objekte durch die Werte der Programmparameter bestimmt werden.

Nachdem dem "Testvirus" ein Präfix hinzugefügt wurde, speichern Sie die Datei z.B. unter dem Namen *eicar_dele.com*. Verwenden Sie die in der Tabelle angegebenen Namen für die modifizierten "Viren".

Table 1. Modifikationen des "Testvirus"

Präfix	Status des Objekts	Informationen zur Verarbeitung des Objekts
Kein Präfix, standardmäßiger "Testvirus".	**Infiziert**. Das Objekt enthält einen bekannten Viruscode. Die Desinfektion ist nicht möglich.	Das Programm identifiziert dieses Objekt als Virus, der nicht desinfiziert werden kann. Beim Desinfektionsversuch des Objekts tritt ein Fehler auf und die für irreparable Objekte geltende Aktion wird ausgeführt.
CORR–	**Beschädigt**.	Das Programm hat Zugriff auf das Objekt erhalten, kann es aber aufgrund einer Beschädigung nicht untersuchen (z.B. beschädigte Struktur des Objekts, ungültiges Dateiformat). Informationen darüber, dass das Objekt verarbeitet wurde, können Sie dem Bericht über die Arbeit der Anwendung entnehmen.
WARN–	**Verdächtig**. Das Objekt enthält einen unbekannten Viruscode. Die Desinfektion ist nicht möglich.	Das Objekt wurde bei der heuristischen Analyse als verdächtig erkannt. Im Augenblick des Funds enthalten die Antiviren-Datenbanken keine Beschreibung zur Desinfektion dieses Objekts. Beim Fund eines solchen Objekts, erhalten Sie eine Meldung.
SUSP–	**Verdächtig**. Das Objekt enthält den modifizierten Code eines bekannten Virus. Die Desinfektion ist nicht möglich.	Das Programm hat erkannt, dass der Objektcode teilweise mit dem Code eines bekannten Virus übereinstimmt. Im Augenblick des Funds enthalten die Antiviren-Datenbanken keine Beschreibung zur Desinfektion dieses Objekts. Beim Fund eines solchen Objekts, erhalten Sie eine Meldung.
ERRO–	**Untersuchungsfehler**.	Bei der Untersuchung des Objekts ist ein Fehler aufgetreten. Die Anwendung erhielt keinen Zugriff auf das Objekt: Die Integrität des Objekts ist beschädigt (z.B. kein Endpunkt in einem Multi-Level-Archiv) oder die Verbindung zu dem Objekt fehlt (wenn ein Objekt in einer Netzwerkressource untersucht wird). Informationen darüber, dass das Objekt verarbeitet wurde, können Sie dem Bericht über die Arbeit der Anwendung entnehmen.
CURE–	**Infiziert**. Das Objekt enthält einen bekannten Viruscode. Die Desinfektion ist möglich.	Das Objekt enthält einen Virus, der desinfiziert werden kann. Das Programm führt die Desinfektion des Objekts aus, wobei der Text des Viruskörpers in CURE geändert wird. Beim Fund eines solchen Objekts, erhalten Sie eine Meldung.
DELE–	**Infiziert**. Das Objekt enthält einen bekannten Viruscode. Die Desinfektion ist nicht möglich.	Das Programm identifiziert dieses Objekt als Virus, der nicht desinfiziert werden kann. Beim Desinfektionsversuch des Objekts tritt ein Fehler auf und die für irreparable Objekte geltende Aktion wird ausgeführt. Beim Fund eines solchen Objekts, erhalten Sie eine Meldung.

TESTEN DES SCHUTZES FÜR HTTP-DATENVERKEHR

Gehen Sie folgendermaßen vor, um die den Virenschutz für den mit HTTP-Protokoll übertragenen Datenverkehr zu prüfen:

Versuchen Sie, den "Testvirus" von der offiziellen Internetseite des **EICAR**-Instituts herunterzuladen: http://www.eicar.org/anti_virus_test_file.htm.

Beim Versuch, den "Testvirus" herunterzuladen, erkennt Kaspersky Internet Security das Objekt, identifiziert es als infiziert und irreparabel, und führt die Aktion aus, die in den Einstellungen für die Untersuchung des HTTP-Datenverkehrs dafür festgelegt wurde. Wenn versucht wird, den "Testvirus" herunterzuladen, wird in der Grundeinstellung die Verbindung mit der Ressource getrennt und im Browserfenster erscheint eine Meldung darüber, dass dieses Objekt von dem Virus EICAR-Test-File infiziert ist.

SCHUTZ FÜR DEN SMTP-DATENVERKEHR TESTEN

Um den Virenschutz für den mit SMTP-Protokoll übertragenen Datenverkehr zu prüfen, können Sie ein Mailprogramm verwenden, das die Daten mit diesem Protokoll überträgt.

Es wird empfohlen, die Arbeit von Anti-Virus für ausgehende E-Mail sowohl im Briefkörper als auch in Anlagen zu testen. Um den Virenschutz im Körper einer E-Mail zu prüfen, fügen Sie den Text des standardmäßigen oder modifizierten "Testvirus" in den Briefkörper ein.

Gehen Sie dazu folgendermaßen vor:

1. Erstellen Sie mit Hilfe des auf Ihrem Computer installierten Mailprogramms eine E-Mail im Format **Gewöhnlicher Text**.

   Eine Nachricht, die den "Testvirus" enthält und das Format RTF oder HTML besitzt, wird nicht untersucht!

2. Fügen Sie den Text des standardmäßigen oder modifizierten "Testvirus" am Anfang der Nachricht ein oder hängen Sie eine Datei, die den "Testvirus" enthält, an die Nachricht an.

3. Schicken Sie die E-Mail an die Adresse des Administrators.

Das Programm erkennt das Objekt, identifiziert es als infiziert und blockiert das Senden der E-Mail.

ÜBERPRÜFUNG DER EINSTELLUNGEN VON DATEI-ANTI-VIRUS

Gehen Sie folgendermaßen vor, um zu prüfen, ob Datei-Anti-Virus korrekt eingestellt wurde:

1. Erstellen Sie einen Ordner auf der Festplatte. Kopieren Sie den von der offiziellen Seite des **EICAR**-Instituts (http://www.eicar.org/anti_virus_test_file.htm) heruntergeladenen "Testvirus" und die von Ihnen erstellten Modifikationen des "Testvirus" in diesen Ordner.

2. Erlauben Sie das Protokollieren aller Ereignisse, damit Daten über beschädigte Objekte oder Objekte, die aufgrund einer Störung nicht untersucht werden, in der Berichtsdatei gespeichert werden.

3. Starten Sie den "Testvirus" oder seine Modifikation zur Ausführung.

Datei-Anti-Virus fängt den Zugriff auf die Datei ab, untersucht sie und führt die in den Einstellungen festgelegte Aktion aus. Durch die Auswahl unterschiedlicher Aktionsvarianten für ein gefundenes Objekt können Sie die Funktion der Komponente vollständig testen.

Vollständige Informationen über die Arbeitsergebnisse von Datei-Anti-Virus sind im Bericht über die Arbeit der Komponente enthalten.

ÜBERPRÜFUNG DER EINSTELLUNGEN FÜR EINE AUFGABE ZUR VIRENSUCHE

Gehen Sie folgendermaßen vor, um zu prüfen, ob eine Aufgabe zur Virensuche korrekt eingestellt wurde:

1. Erstellen Sie einen Ordner auf der Festplatte. Kopieren Sie den von der offiziellen Seite des **EICAR**-Instituts http://www.eicar.org/anti_virus_test_file.htm) heruntergeladenen "Testvirus" und die von Ihnen erstellten Modifikationen des "Testvirus" in diesen Ordner.

2. Erstellen Sie eine neue Untersuchungsaufgabe und wählen Sie als Untersuchungsobjekt den Ordner, der die "Testviren" enthält.

3. Erlauben Sie das Protokollieren aller Ereignisse, damit Daten über beschädigte Objekte oder Objekte, die aufgrund einer Störung nicht untersucht werden, in der Berichtsdatei gespeichert werden.

4. Starten Sie die Ausführung der Untersuchungsaufgabe.

Wenn bei der Untersuchung verdächtige oder infizierte Objekte gefunden werden, werden die in den Einstellungen der Aufgabe festgelegten Aktionen ausgeführt. Durch die Auswahl unterschiedlicher Aktionsvarianten für ein gefundenes Objekt können Sie die Funktion der Komponente vollständig testen.

Vollständige Informationen über das Ausführungsergebnis der Untersuchungsaufgabe sind im Bericht über die Arbeit der Komponente enthalten.

ÜBERPRÜFUNG DER EINSTELLUNGEN FÜR DEN SCHUTZ VOR UNERWÜNSCHTEN E-MAILS

Zur Überprüfung des Schutzes vor unerwünschten E-Mails können Sie eine Testnachricht verwenden, die vom Programm als Spam identifiziert wird.

Die Testnachricht muss folgenden Text in der Betreffzeile enthalten:

```
Spam is bad do not send it
```

Nachdem diese Nachricht auf dem Computer eingetroffen ist, untersucht Kaspersky Internet Security sie, stuft sie als Spam ein und führt die Aktion damit aus, die für diesen Objekttyp festgelegt wurde.

BEDIENUNG DES PROGRAMMS ÜBER DIE BEFEHLSZEILE

Sie können Kaspersky Internet Security mit Hilfe der Befehlszeile steuern. Dabei ist die Möglichkeit zum Ausführen der folgenden Operationen vorgesehen:

- Programmkomponenten starten und beenden.
- Ausführung von Untersuchungsaufgaben starten und beenden.
- Erhalt von Informationen über den aktuellen Status von Komponenten und Aufgaben und ihrer Statistik.
- Untersuchung von ausgewählten Objekten.
- Update der Datenbanken und Module des Programms.
- Aufruf der Hilfe über die Syntax der Befehlszeile.
- Aufruf der Hilfe über die Syntax eines Befehls.

Syntax der Befehlszeile:

```
avp.com <Befehl> [Parameter]
```

Der Zugriff auf das Programm über die Befehlszeile muss aus dem Installationsordner des Produkts oder unter Angabe des vollständigen Pfads von avp.com erfolgen.

Es sind folgende Befehle vorgesehen:

ACTIVATE	Aktivierung von Kaspersky Internet Security über das Internet mit Hilfe eines Aktivierungscodes
ADDKEY	Programmaktivierung mit Hilfe einer Lizenzschlüsseldatei (die Ausführung des Befehls ist nur möglich, wenn das Kennwort eingegeben wird, das über die Programmoberfläche festgelegt wurde)
START	Komponente oder Aufgabe starten
STOP	Beenden der Arbeit einer Komponente oder Aufgabe (die Ausführung des Befehls ist nur möglich, wenn das Kennwort eingegeben wird, das auf dem Interface von Kaspersky Internet Security festgelegt wurde)
STATUS	Bildschirmanzeige des aktuellen Status einer Komponente oder Aufgabe
STATISTICS	Bildschirmanzeige der Statistik über die Arbeit einer Komponente oder Aufgabe
HELP	Hilfe über die Befehlssyntax, Anzeige einer Befehlsliste
SCAN	Untersuchung von Objekten auf das Vorhandensein von Viren
UPDATE	Programm-Update starten
ROLLBACK	Rückgängigmachen des zuletzt durchgeführten Updates von Kaspersky Internet Security (die Ausführung des Befehls ist nur möglich, wenn das Kennwort eingegeben wird, das über die Programmoberfläche festgelegt

	wurde)
EXIT	Beenden der Arbeit mit dem Programm (dieser Befehl kann nur ausgeführt werden, wenn das über die Programmoberfläche festgelegte Kennwort angegeben wird)
IMPORT	Importieren von Schutzeinstellungen für Kaspersky Internet Security (die Ausführung des Befehls ist nur möglich, wenn über die Programmoberfläche festgelegte Kennwort angegeben wird)
EXPORT	Schutzparameter des Programms exportieren

Jedem Befehl entspricht eine eigene Auswahl von Parametern, die für eine konkrete Komponente des Programms spezifisch sind.

IN DIESEM ABSCHNITT

Programm aktivieren 221

Steuerung von Komponenten und Aufgaben des Programms 222

Virensuche 224

Programm-Update 227

Rollback zum vorherigen Update 227

Schutzparameter exportieren 228

Schutzparameter importieren 228

Programm starten 229

Programm beenden 229

Protokolldatei anlegen 229

Hilfe anzeigen 230

Rückgabecodes der Befehlszeile 230

PROGRAMM AKTIVIEREN

Die Aktivierung von Kaspersky Internet Security kann auf zwei Arten erfolgen:

- über das Internet mit Hilfe eines Aktivierungscodes (Befehl ACTIVATE)
- mit Hilfe einer Schlüsseldatei (Befehl ADDKEY).

Befehlssyntax:

```
ACTIVATE <Aktivierungscode>
ADDKEY <Dateiname> /password=<Kennwort>
```

Beschreibung der Parameter:

<Aktivierungscode>	Aktivierungscode für das Programm, den Sie beim Kauf der Lizenz erhalten haben.
<Dateiname>	Name der Lizenzschlüsseldatei für das Programm (Endung **.key*).
<Kennwort>	Kennwort für das Programm, das über die Programmoberfläche festgelegt wurde.

Der Befehl **ADDKEY** wird nur ausgeführt, wenn das Kennwort eingegeben wird.

Beispiel:

```
avp.com ACTIVATE 11AA1-11AAA-1AA11-1A111
avp.com ADDKEY 1AA111A1.key /password=<Kennwort>
```

STEUERUNG VON KOMPONENTEN UND AUFGABEN DES PROGRAMMS

Befehlssyntax:

```
avp.com <Befehl> <Profil|Aufgabenname> [/R[A]:<Berichtsdatei>]
avp.com STOP|PAUSE <Profil|Aufgabenname>  /password=<Kennwort> [/R[A]:<Berichtsdatei>]
```

<Befehl>	Die Steuerung der Komponenten und Aufgaben von Kaspersky Internet Security wird mit Hilfe der folgenden Befehle ausgeführt: START – Start einer Schutzkomponente oder einer Aufgabe. STOP – Beenden einer Schutzkomponente oder einer Aufgabe. STATUS – Aktuellen Status einer Komponente oder Aufgabe auf dem Bildschirm anzeigen. STATISTICS – Die Statistik über die Arbeit einer Schutzkomponente oder einer Aufgabe auf dem Bildschirm anzeigen. Beachten Sie, dass der Befehl STOP nur ausgeführt wird, wenn das Kennwort eingegeben wird.
<Profil|Aufgabenname>	Als Wert für den Parameter **<Profil>** sind möglich: eine beliebige Schutzkomponente von Kaspersky Internet Security, Module, die zu den Komponenten gehören, erstellte Untersuchungs- oder Updateaufgaben (die vom Programm standardmäßig verwendeten Werte werden in folgender Tabelle genannt). Als Wert für den Parameter **<Aufgabenname>** kann der Name einer beliebigen vom Benutzer erstellten Untersuchungs- oder Updateaufgabe angegeben werden.
<Kennwort>	Kennwort für das Programm, das über die Programmoberfläche festgelegt wurde.

/R[A]:<Berichtsdatei>	**/R:<Berichtsdatei>** – nur wichtige Ereignisse im Bericht protokollieren. **/RA:<Berichtsdatei>** - alle Ereignisse im Bericht protokollieren. Die Angabe des absoluten oder relativen Pfads der Datei ist zulässig. Wenn der Parameter nicht angegeben wird, werden die Untersuchungsergebnisse auf dem Bildschirm angezeigt, alle Ereignisse werden angezeigt.

Für den Parameter **<Profil>** wird einer der folgenden Werte angegeben:

RTP	Alle Schutzkomponenten. Der Befehl **avp.com START RTP** startet alle Schutzkomponenten, wenn der Schutz vollständig deaktiviert war. Wenn eine Komponente mit dem Befehl **STOP** aus der Befehlzeile beendet wurde, wird sie durch den Befehl **avp.com START RTP** nicht gestartet. Um die Komponente zu starten, ist der Befehl **avp.com START <Profil>** erforderlich, wobei als **<Profil>** der Wert der betreffenden Schutzkomponente verwendet wird, beispielsweise **avp.com START FM**.
FW	Firewall
HIPS	Programmkontrolle
pdm	Proaktiver Schutz
FM	Datei-Anti-Virus
EM	Mail-Anti-Virus
WM	Web-Anti-Virus Werte für die Subkomponenten von Web-Anti-Virus: **httpscan (HTTP)** – Untersuchung des http-Datenstroms **sc** – Skript-Untersuchung
IM	IM-Anti-Virus
AB	Anti-Banner
AS	Anti-Spam
PC	Kindersicherung
AP	Anti-Phishing
ids	Schutz vor Netzwerkangriffen
Updater	Update
Rollback	Rollback zum vorherigen Update
Scan_My_Computer	Untersuchung des Computers
Scan_Objects	Untersuchung von Objekten

Scan_Quarantine	Quarantäne untersuchen
Scan_Rootkits	Nach Rootkits (rootkit) suchen
Scan_Startup (STARTUP)	Autostart-Objekte untersuchen
Scan_Vulnerabilities (SECURITY)	Suche nach Schwachstellen

Die aus der Befehlszeile gestarteten Komponenten und Aufgaben werden mit den Parametern ausgeführt, die über die Programmoberfläche festgelegt wurden.

Beispiele:

- *Um Datei-Anti-Virus zu aktivieren, geben Sie in der Befehlszeile ein:*

```
avp.com START FM
```

- *Um die Arbeit der Kindersicherung fortzusetzen, geben Sie in der Befehlszeile ein:*

```
avp.com RESUME ParCtl
```

- *Um die Aufgabe zur Untersuchung des Computers zu beenden, geben Sie in der Befehlszeile ein:*

```
avp.com STOP Scan_My_Computer /password=<Kennwort>
```

VIRENSUCHE

Die Befehlszeile zum Starten der Virenuntersuchung eines bestimmten Bereichs und zur Verarbeitung von schädlichen Objekten besitzt folgendes allgemeines Aussehen:

```
avp.com SCAN [<Untersuchungsobjekt>] [<Aktion>] [<Dateitypen>] [<Ausnahmen>]
[<Konfigurationsdatei>] [<Berichtsparameter>] [<zusätzliche Parameter>]
```

Für die Untersuchung von Objekten können Sie auch die im Programm erstellten Aufgaben verwenden, die aus der Befehlszeile gestartet werden können. Dabei wird die Aufgabe mit den Parametern ausgeführt, die über die Oberfläche von Kaspersky Internet Security festgelegt wurden.

Beschreibung der Parameter:

<Untersuchungsobjekt> – Der Parameter gibt eine Liste der Objekte an, die auf das Vorhandensein von schädlichem Code untersucht werden sollen. Der Parameter kann mehrere Werte aus der folgenden Liste enthalten. Die Werte werden durch Leerzeichen getrennt.	
<files>	Liste mit den Pfaden der Dateien und / oder Ordner für die Untersuchung. Die Angabe des absoluten oder relativen Pfads der Datei ist zulässig. Als Trennzeichen für die Elemente der Liste dient das Leerzeichen. Kommentare: • Wenn der Objektname ein Leerzeichen enthält, wird er in Anführungszeichen gesetzt. • Wenn ein konkreter Ordner angegeben wird, werden alle darin enthaltenen Dateien untersucht.
/MEMORY	Objekte des Arbeitsspeichers.

/STARTUP	Autostart-Objekte**.**
/MAIL	Posteingänge.
/REMDRIVES	Alle Wechseldatenträger.
/FIXDRIVES	Alle lokalen Laufwerke.
/NETDRIVES	Alle Netzlaufwerke.
/QUARANTINE	Objekte in Quarantäne.
/ALL	Vollständige Untersuchung des Computers.
/@:<filelist.lst>	Pfad der Datei mit einer Liste der Objekte und Ordner, die untersucht werden sollen. Die Datei muss das Textformat besitzen. Jedes Untersuchungsobjekt muss in einer separaten Zeile stehen. Die Angabe des absoluten oder relativen Pfads der Datei ist zulässig. Der Pfad wird ohne Anführungszeichen angegeben, selbst wenn er ein Leerzeichen enthält.
<Aktion> – Der Parameter bestimmt die Aktionen mit einem schädlichen Objekt, das während der Untersuchung gefunden wird. Wenn der Parameter nicht angegeben wird, wird standardmäßig die Aktion ausgeführt, die dem Wert **/i8** entspricht.	
/i0	Keine Aktion ausführen, nur Informationen im Bericht protokollieren.
/i1	infizierte Objekte desinfizieren; wenn die Desinfektion nicht möglich ist – überspringen**.**
/i2	Infizierte Objekte desinfizieren; wenn die Desinfektion nicht möglich ist – löschen; infizierte Objekte aus Containern (zusammengesetzten Objekten) nicht löschen; Container mit ausführbarer Kopfzeile (sfx-Archive) löschen.
/i3	infizierte Objekte desinfizieren; wenn die Desinfektion nicht möglich ist – löschen; Container-Objekte vollständig löschen, wenn die darin enthaltenen infizierten Dateien nicht gelöscht werden können.
/i4	infizierte Objekte löschen; Container-Objekte vollständig löschen, wenn die darin enthaltenen infizierten Dateien nicht gelöscht werden können.
/i8	Beim Fund eines infizierten Objekts den Benutzer nach der Aktion fragen.
/i9	Den Benutzer nach der Aktion fragen, wenn die Untersuchung abgeschlossen wird.
<Dateitypen> – Der Parameter bestimmt die Typen der Dateien, die der Virenuntersuchung unterzogen werden. Wenn der Parameter nicht angegeben wird, werden standardmäßig nur infizierbare Dateien nach ihrem Inhalt untersucht.	
/fe	Nur infizierbare Dateien nach Erweiterung untersuchen.
/fi	Nur infizierbare Dateien nach Inhalt untersuchen.
/fa	**Alle Dateien untersuchen**.
<Ausnahmen> – Der Parameter bestimmt die Objekte, die von der Untersuchung ausgeschlossen werden sollen. Der Parameter kann mehrere Werte aus der folgenden Liste enthalten. Die Werte werden durch Leerzeichen getrennt.	
-e:a	Archive nicht untersuchen.

-e:b	Mail-Datenbanken nicht untersuchen.
-e:m	E-Mail-Nachrichten im Format plain text nicht untersuchen.
-e:<filemask>	Objekte nach Maske nicht untersuchen.
-e:<seconds>	Objekte überspringen, deren Untersuchung länger dauert, als der durch den Parameter **<seconds>** angegebene Zeitraum.
-es:<size>	Objekte überspringen, deren Größe (in MB) über dem Wert liegt, der durch den Parameter **<size>** angegeben wird.
<Konfigurationsdatei> – bestimmt den Pfad der Konfigurationsdatei, in der die Parameter für die Arbeit des Programms bei der Untersuchung enthalten sind. Die Konfigurationsdatei ist eine Datei im Textformat, die eine Auswahl von Befehlszeilenparametern für die Antiviren-Untersuchung enthält. Die Angabe des absoluten oder relativen Pfads der Datei ist zulässig. Wenn der Parameter nicht angegeben wird, werden die Werte verwendet, die über die Programmoberfläche festgelegt wurden.	
/C:<Dateiname>	Die Werte der Parameter, die in der Datei **<Dateiname>** angegeben sind, verwenden.
<Berichtsparameter> – Der Parameter bestimmt das Format des Berichts über die Untersuchungsergebnisse. Die Angabe des absoluten oder relativen Pfads der Datei ist zulässig. Wenn der Parameter nicht angegeben wird, werden die Untersuchungsergebnisse auf dem Bildschirm angezeigt, alle Ereignisse werden angezeigt.	
/R:<Berichtsdatei>	Nur wichtige Ereignisse in der angegebenen Berichtsdatei protokollieren.
/RA:<Berichtsdatei>	Alle wichtigen Ereignisse in der angegebenen Berichtsdatei protokollieren.
<zusätzliche Parameter> – Parameter, der die Verwendung von Technologien zur Virenuntersuchung festlegt.	
/iChecker=<on|off>	Verwendung der Technologie iChecker aktivieren / deaktivieren.
/iSwift=<on|off>	Verwendung der Technologie iSwift aktivieren / deaktivieren.

Beispiele:

- *Untersuchung des Arbeitsspeichers, der Autostart-Objekte, der Mailboxen sowie der Ordner Eigene Dateien, Programme und der Datei test.exe:*

```
avp.com SCAN /MEMORY /STARTUP /MAIL "C:\Dokumente und Einstellungen\All Users\Eigene Dateien" "C:\Programme" "C:\Downloads\test.exe"
```

- *Anhalten der Untersuchung von ausgewählten Objekten, Startender vollständigen Untersuchung des Computers, bei Abschluss der Untersuchung soll die Virensuche in den ausgewählten Objekten fortgesetzt werden:*

```
avp.com PAUSE Scan_Objects /password=<Kennwort>
avp.com START Scan_My_Computer
avp.com RESUME Scan_Objects
```

- *Untersuchung der Objekte, deren Liste in der Datei object2scan.txt angegeben ist. Für die Arbeit soll die Konfigurationsdatei scan_setting.txt verwendet werden. Über die Untersuchungsergebnisse soll ein Bericht erstellt werden, in dem alle Ereignisse aufgezeichnet werden:*

```
avp.com SCAN /MEMORY /@:objects2scan.txt /C:scan_settings.txt /RA:scan.log
```

Beispiel für die Konfigurationsdatei:

```
/MEMORY /@:objects2scan.txt /C:scan_settings.txt /RA:scan.log
```

PROGRAMM-UPDATE

Der Befehl für das Update der Programm-Module und Datenbanken von Kaspersky Internet Security besitzt folgende Syntax:

```
avp.com UPDATE [<Updatequelle>] [/R[A]:<Berichtsdatei>] [/C:<Dateiname>]
[/APP=<on|off>]
```

Beschreibung der Parameter:

<Updatequelle>	HTTP-, FTP-Server oder Netzwerkordner für den Download von Updates. Als Wert für diesen Parameter kann der vollständige Pfad oder die URL-Adresse der Updatequelle angegeben werden. Wenn der Pfad nicht angegeben wird, wird die Updatequelle aus den Parametern des Diensts für das Programm-Update übernommen.
/R[A]:<Berichtsdatei>	**/R:<Berichtsdatei> –** nur wichtige Ereignisse im Bericht protokollieren. **/RA:<Berichtsdatei> –** alle Ereignisse im Bericht protokollieren. Die Angabe des absoluten oder relativen Pfads der Datei ist zulässig. Wenn der Parameter nicht angegeben wird, werden die Untersuchungsergebnisse auf dem Bildschirm angezeigt, alle Ereignisse werden angezeigt.
/C:<Dateiname>	Pfad der Konfigurationsdatei, die die Parameter für die Arbeit von Kaspersky Internet Security beim Update enthält. Die Konfigurationsdatei ist eine Textdatei, die eine Auswahl von Befehlszeilenparametern für das Update des Programms enthält. Die Angabe des absoluten oder relativen Pfads der Datei ist zulässig. Wenn der Parameter nicht angegeben wird, werden die Werte verwendet, die über die Programmoberfläche festgelegt wurden.
/APP=<on|off>	Update der Programm-Module aktivieren / deaktivieren.

Beispiele:

- *Update der Programm-Datenbanken, alle Ereignisse im Bericht protokollieren:*

  ```
  avp.com UPDATE /RA:avbases_upd.txt
  ```

- *Update der Programm-Module von Kaspersky Internet Security, die Parameter der Konfigurationsdatei updateapp.ini verwenden:*

  ```
  avp.com UPDATE /APP=on /C:updateapp.ini
  ```

Beispiel für die Konfigurationsdatei:

```
"ftp://my_server/kav updates" /RA:avbases_upd.txt /app=on
```

ROLLBACK ZUM VORHERIGEN UPDATE

Befehlssyntax:

```
ROLLBACK [/R[A]:<Berichtsdatei>] [/password=<Kennwort>]
```

Beschreibung der Parameter:

/R[A]:<Berichtsdatei>	**/R:<Berichtsdatei> –** nur wichtige Ereignisse im Bericht protokollieren. **/RA:<Berichtsdatei> –** alle Ereignisse im Bericht protokollieren.

	Die Angabe des absoluten oder relativen Pfads der Datei ist zulässig. Wenn der Parameter nicht angegeben wird, werden die Untersuchungsergebnisse auf dem Bildschirm angezeigt, alle Ereignisse werden angezeigt.
<Kennwort>	Kennwort für das Programm, das über die Programmoberfläche festgelegt wurde.

Beachten Sie, dass dieser Befehl nicht ausgeführt wird, wenn das Kennwort nicht eingegeben wird.

Beispiel:

```
avp.com ROLLBACK /RA:rollback.txt /password=<Kennwort>
```

SCHUTZPARAMETER EXPORTIEREN

Befehlssyntax:

```
avp.com EXPORT <Profil> <Dateiname>
```

Beschreibung der Parameter:

<Profil>	Komponente oder Aufgabe, für die der Export von Parametern ausgeführt wird. Als Wert des Parameters **<Profil>** kann ein beliebiger Wert dienen, der im Hilfeabschnitt "Steuerung von Komponenten und Aufgaben des Programms" genannt wird.
<Dateiname>	Pfad der Datei, in welche die Parameter von Kaspersky Internet Security exportiert werden. Ein absoluter oder relativer Pfad kann angegeben werden. Die Konfigurationsdatei wird im Binärformat (*dat*) gespeichert und kann künftig verwendet werden, um die Einstellungen des Programms auf andere Computer zu übertragen. Außerdem können Sie die Konfigurationsdatei im Textformat speichern. Geben Sie dazu im Dateinamen die Endung *txt* an. Beachten Sie, dass der Import von Schutzparametern aus einer Textdatei nicht unterstützt wird. Diese Datei kann nur zur Ansicht der grundlegenden Funktionsparameter von Kaspersky Internet Security verwendet werden.

Beispiel:

```
avp.com EXPORT c:\settings.dat
```

SCHUTZPARAMETER IMPORTIEREN

Befehlssyntax:

```
avp.com IMPORT <Dateiname> [/password=<Kennwort>]
```

<Dateiname>	Pfad der Datei, aus welcher die Parameter von Kaspersky Internet Security importiert werden. Ein absoluter oder relativer Pfad kann angegeben werden.
<Kennwort>	Kennwort für Kaspersky Internet Security, das über die Programmoberfläche festgelegt wurde. <Kennwort>

Beachten Sie, dass dieser Befehl nicht ausgeführt wird, wenn das Kennwort nicht eingegeben wird.

Beispiel:

```
avp.com IMPORT c:\settings.dat /password=<Ihr_Kennwort>
```

PROGRAMM STARTEN

Befehlssyntax:

```
avp.com
```

PROGRAMM BEENDEN

Befehlssyntax:

```
EXIT /password=<Kennwort>
```

<Kennwort>	Kennwort für das Programm, das über die Programmoberfläche festgelegt wurde.

Beachten Sie, dass dieser Befehl nicht ausgeführt wird, wenn das Kennwort nicht eingegeben wird.

PROTOKOLLDATEI ANLEGEN

Das Anlegen einer Protokolldatei kann erforderlich sein, wenn bei der Arbeit mit Kaspersky Internet Security Probleme auftreten, deren genaue Analyse durch die Experten des technischen Supports notwendig ist.

Befehlssyntax:

```
avp.com TRACE [file] [on|off] [<Tracing-Niveau>]
```

Beschreibung der Parameter:

[on|off]	Anlegen einer Protokolldatei aktivieren / deaktivieren.
[file]	Tracing in Form einer Datei erstellen.
<Tracing-Niveau>	Für diesen Parameter kann ein Zahlenwert im Bereich von 0 (minimale Stufe, nur kritische Meldungen) bis 700 (maximale Stufe, alle Meldungen) festgelegt werden. Wenn Sie sich an den technischen Support wenden, nennt Ihnen der zuständige Spezialist das erforderliche Tracing-Niveau. Andernfalls gilt das Niveau 500 als empfehlenswert.

Es wird empfohlen, das Anlegen von Tracing-Dateien nur zur Diagnose eines konkreten Problems zu aktivieren. Sollte das Tracing ständig aktiv sein, so kann die Leistungsfähigkeit des Computers sinken und es kann zur Überfüllung der Festplatte kommen.

Beispiele:

- *Erstellen von Protokolldateien deaktivieren:*

```
avp.com TRACE file off
```

- *Erstellen einer Tracing-Datei zum Senden an den technischen Support, mit einem maximalen Tracing-Niveau von 500:*

```
avp.com TRACE file on 500
```

HILFE ANZEIGEN

Zur Anzeige der Hilfe über die Syntax der Befehlzeile dient folgender Befehl:

```
avp.com [ /? | HELP ]
```

Um Hilfe über die Syntax eines konkreten Befehls zu erhalten, können Sie einen der folgenden Befehle verwenden:

```
avp.com <Befehl> /?
avp.com HELP <Befehl>
```

RÜCKGABECODES DER BEFEHLSZEILE

In diesem Abschnitt werden die Rückgabecodes der Befehlszeile beschrieben. Die allgemeinen Codes können von einem beliebigen Befehl der Befehlszeile zurückgegeben werden. Als Rückgabecodes für Aufgaben sind die allgemeinen Codes sowie spezifische Codes für einen konkreten Aufgabentyp möglich.

ALLGEMEINE RÜCKGABECODES	
0	Operation wurde erfolgreich ausgeführt
1	Ungültiger Parameterwert
2	Unbekannter Fehler
3	Fehler bei Ausgabenausführung
4	Aufgabenausführung wurde abgebrochen
RÜCKGABECODES FÜR AUFGABEN ZUR VIRENSUCHE	
101	Alle gefährlichen Objekte wurden bearbeitet
102	Es wurden gefährliche Objekte gefunden

PROBLEME BEHEBEN

Wenn bei der Verwendung von Kaspersky Internet Security Probleme aufgetreten sind, prüfen Sie bitte zuerst, ob das Hilfesystem oder die Wissensdatenbank von Kaspersky Lab eine Lösung für Ihr Problem bieten (http://support.kaspersky.com/de). Die *Wissensdatenbank* ist ein Abschnitt der Webseite des technischen Support-Services und enthält Tipps über die Arbeit mit Kaspersky-Lab-Produkten und Antworten auf häufige Fragen. Versuchen Sie, auf dieser Webseite eine Antwort auf Ihre Frage oder eine Lösung für Ihr Problem zu finden.

Gehen Sie folgendermaßen vor, um die Wissensdatenbank zu verwenden:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im unteren Bereich des Fensters auf den Link **Support**.
3. Klicken Sie im folgenden Fenster **Support** auf den Link **Wissensdatenbank**.

Eine weitere Quelle, die Informationen über die Arbeit mit der Anwendung bietet, ist das Benutzerforum für Kaspersky-Lab-Produkte. Das Forum ist ebenfalls ein Abschnitt der Webseite des technischen Support Services und enthält Fragen, Kommentare und Vorschläge von Programmbenutzern. Sie können die wichtigsten Themen des Forums kennen lernen, eigene Beiträge über das Programm schreiben oder Antworten auf Ihre Frage suchen.

Gehen Sie folgendermaßen vor, um die Webseite des Benutzerforums zu öffnen:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im unteren Bereich des Fensters auf den Link **Support**.
3. Klicken Sie im folgenden Fenster **Support** auf den Link **Benutzerforum**.

Wenn Sie im Hilfesystem, in der Wissensdatenbank oder im Benutzerforum keine Lösung für Ihr Problem finden können, empfehlen wir Ihnen, sich an den technischen Support von Kaspersky Lab zu wenden.

IN DIESEM ABSCHNITT

Bericht über den Systemzustand erstellen 231

Protokolldatei erstellen 232

Dateien mit Daten senden 232

AVZ-Skript ausführen 233

BERICHT ÜBER DEN SYSTEMZUSTAND ERSTELLEN

Damit die Support-Spezialisten von Kaspersky Lab Sie bei der Lösung eines Problems unterstützen können, kann es erforderlich sein, einen Bericht über den Zustand des Systems zu erstellen. Dieser Bericht enthält ausführliche Informationen über gestartete Prozesse, geladene Module und Treiber, Erweiterungsmodule für Microsoft Internet Explorer und Microsoft Windows Explorer, offene Ports, gefundene verdächtige Objekte u.a.

Beim Erstellen des Berichts über den Systemzustand werden keine persönlichen Benutzerdaten gesammelt.

Gehen Sie folgendermaßen vor, um einen Bericht über den Systemzustand zu erstellen:

1. Öffnen Sie das Programmhauptfenster.

2. Klicken Sie im unteren Bereich des Programmfensters auf den Link **Support**.

3. Klicken Sie im folgenden Fenster **Support** auf den Link **Protokollierung**.

4. Im folgenden Fenster **Informationen für den Support** klicken Sie auf die Schaltfläche **Bericht über den Systemstatus erstellen**.

Der Bericht über den Systemzustand wird in den Formaten *html* und *xml* erstellt und im Archiv *sysinfo.zip* gespeichert. Nachdem das Sammeln von Daten über das System abgeschlossen wurde, können Sie einen Bericht ansehen.

Gehen Sie folgendermaßen vor, um einen Bericht anzuzeigen:

1. Öffnen Sie das Programmhauptfenster.

2. Klicken Sie im unteren Bereich des Programmfensters auf den Link **Support**.

3. Klicken Sie im folgenden Fenster **Support** auf den Link **Protokollierung**.

4. Im folgenden Fenster **Informationen für den Support** klicken Sie auf die Schaltfläche **Anzeigen**.

5. Öffnen Sie das Archiv *sysinfo.zip*, das die Protokolldateien enthält.

PROTOKOLLDATEI ERSTELLEN

Nach der Installation von Kaspersky Internet Security können bei der Arbeit des Betriebssystems oder bestimmter Programme Störungen auftreten. Dies deutet höchstwahrscheinlich auf einen Konflikt von Kaspersky Internet Security mit einem Programm, das auf Ihrem Computer installiert ist, oder mit auf Ihrem Computer vorhandenen Treibern hin. Damit die Support-Spezialisten von Kaspersky Lab Sie bei der Lösung Ihres Problems unterstützen können, kann es sein, dass der Support Sie auffordert, eine Protokolldatei zu erstellen.

Gehen Sie folgendermaßen vor, um eine Protokolldatei zu erstellen:

1. Öffnen Sie das Programmhauptfenster.

2. Klicken Sie im unteren Bereich des Programmfensters auf den Link **Support**.

3. Klicken Sie im folgenden Fenster **Support** auf den Link **Protokollierung**.

4. Verwenden Sie im folgenden Fenster **Informationen für den Support** die Dropdown-Liste im Block **Protokollierung**, um ein Protokollierungsniveau auszuwählen. Das Tracing-Niveau wird von dem Support-Spezialisten angegeben. Sollte diese Angabe des Supports fehlen, dann empfohlen, das Tracing-Niveau **500** einzustellen.

5. Klicken Sie auf die Schaltfläche **Aktivieren**, um den Protokollierungsvorgang zu starten.

6. Wiederholen Sie die Situation, in der das Problem aufgetreten ist.

7. Klicken Sie auf die Schaltfläche **Deaktivieren**, um den Protokollierungsvorgang zu beenden.

Sie können mit dem Hochladen der Protokollierungsergebnisse (s. Abschnitt "Datendateien versenden" auf S. 232) auf den Server von Kaspersky Lab beginnen.

DATEIEN MIT DATEN SENDEN

Nachdem die Protokolldateien und der Bericht über den Systemzustand erstellt wurden, müssen diese an den technischen Support von Kaspersky Lab geschickt werden.

Um die Dateien mit den Daten auf den Server des technischen Supports hochzuladen, benötigen Sie eine

Anfragenummer. Diese Nummer erhalten Sie in Ihrem Kaspersky Account auf der Seite des technischen Supports, wenn eine aktive Anfrage vorliegt.

Gehen Sie folgendermaßen vor, um die Dateien mit den Daten auf den Server des technischen Supports hochzuladen:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im unteren Bereich des Programmfensters auf den Link **Support**.
3. Klicken Sie im folgenden Fenster **Support** auf den Link **Protokollierung**.
4. Im folgenden Fenster **Informationen für den Support** im Block **Aktionen** klicken Sie auf die Schaltfläche **Informationen für den Support auf den Server hochladen**.
5. Aktivieren Sie im folgenden Fenster die Kontrollkästchen neben den Dateien, die Sie an den technischen Support schicken möchten, und klicken Sie auf die Schaltfläche **Senden**.
6. Im folgenden Fenster **Ticket-Nummer eingeben** geben Sie die Nummer an, die für Ihre Anfrage vergeben wurde, als Sie das elektronische Formular auf der Seite des technischen Supports ausgefüllt haben.

Die ausgewählten Dateien werden komprimiert und an den Server des technischen Supports gesendet.

Falls es nicht möglich ist, Kontakt mit dem technischen Support aufzunehmen, können Sie die Dateien mit Daten auf Ihrem Computer speichern.

Gehen Sie folgendermaßen vor, um die Dateien mit Daten auf der Festplatte zu speichern:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im unteren Bereich des Programmfensters auf den Link **Support**.
3. Klicken Sie im folgenden Fenster **Support** auf den Link **Protokollierung**.
4. Im folgenden Fenster **Informationen für den Support** im Block **Aktionen** klicken Sie auf die Schaltfläche **Informationen für den Support auf den Server hochladen**.
5. Aktivieren Sie im folgenden Fenster die Kontrollkästchen neben den Dateien, die Sie an den technischen Support schicken möchten, und klicken Sie auf die Schaltfläche **Senden**.
6. Im folgenden Fenster **Anfragenummer angeben** klicken Sie auf die Schaltfläche **Abbrechen** und im folgenden Fenster bestätigen Sie das Speichern der Dateien auf dem Datenträger.
7. Geben Sie im folgenden Fenster einen Namen für das Archiv an.

Sie können daraufhin die gespeicherten Dateien an den technischen Support schicken.

AVZ-SKRIPT AUSFÜHREN

Die Spezialisten von Kaspersky Lab analysieren Ihr Problem auf der Grundlage von Protokolldateien und eines Berichts über den Systemzustand. Das Ergebnis der Analyse besteht aus einer Reihe von Aktionen, die dazu dienen, die gefundenen Probleme zu beheben. Oft handelt es sich dabei um sehr viele Aktionen.

Um die Problembehebung zu vereinfachen, werden AVZ-Skripts verwendet. Ein AVZ-Skript ist eine Kombination von Befehlen, die es erlauben, Registrierungsschlüssel zu ändern, Dateien in die Quarantäne zu verschieben, eine Klassensuche mit der Möglichkeit der Isolierung von damit verbundenen Dateien vorzunehmen, Hooks der Typen UserMode und KernelMode zu blockieren, u.a.

Zum Starten der Skripts bietet das Programm einen *Assistenten zum Ausführen von AVZ-Skripts*. Der Assistent besteht aus einer Folge von Fenstern (Schritten). Zur Navigation zwischen den Fenstern dienen die Schaltflächen **Zurück** und

Weiter, zum Abschluss des Assistenten die Schaltfläche **Beenden**. Die Arbeit des Assistenten kann auf einer beliebigen Etappe durch Klick auf die Schaltfläche **Abbrechen** beendet werden.

Es wird davor gewarnt, den Text eines Skripts, das Ihnen von den Support-Spezialisten geschickt wurde, zu verändern. Sollten bei der Skript-Ausführung Probleme auftreten, dann wenden Sie sich an den technischen Support.

Gehen Sie folgendermaßen vor, den Assistenten zu starten:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im unteren Bereich des Programmfensters auf den Link **Support**.
3. Im folgenden Fenster **Support** klicken Sie auf den Link **Protokollierung** im unteren Bereich des Fensters.
4. Im folgenden Fenster **Informationen für den Support** klicken Sie auf die Schaltfläche **AVZ-Skript ausführen**.

Wenn das Skript erfolgreich ausgeführt wurde, wird die der Assistent abgeschlossen. Falls bei der Skript-Ausführung Störungen auftreten, zeigt der Assistent eine entsprechende Meldung an.

ERKLÄRUNG ZUR VERWENDUNG VON KASPERSKY SECURITY NETWORK

A. EINFÜHRUNG

Bitte lesen Sie dieses Dokument sorgfältig. Es enthält wichtige Informationen, die Sie kennen sollten, bevor Sie mit der Nutzung unserer Dienstleistungen oder Software fortfahren. Wenn Sie weiterhin Kaspersky Lab-Software oder –Dienste nutzen, wird davon ausgegangen, dass Sie diese Erklärung zur Datensammlung von Kaspersky Lab akzeptieren. Wir behalten uns das Recht vor, diese Erklärung zur Datensammlung jederzeit durch Veröffentlichung der Änderungen auf dieser Seite zu ändern. Bitte prüfen Sie das untenstehende Änderungsdatum, um festzustellen, ob der Inhalt sich geändert hat, seit Sie ihn zuletzt gelesen haben. Wenn Sie irgendeinen Teil der Kaspersky Lab-Dienste nach der Veröffentlichung der aktualisierten Erklärung zur Datensammlung nutzen, bedeutet dies, dass Sie mit den Änderungen einverstanden sind.

Kaspersky Lab und seine verbundenen Unternehmen (gemeinsam „Kaspersky Lab“ genannt) haben diese Erklärung zur Datensammlung verfasst, um über ihre Vorgehensweise bei der Sammlung und Nutzung von Daten in Zusammenhang mit den Programmen Kaspersky Anti-Virus und Kaspersky Internet Security zu informieren und sie offenzulegen.

Vorbemerkung

Kaspersky Lab ist stets bestrebt, allen seinen Kunden hervorragenden Service zu bieten und insbesondere Ihre etwaigen Bedenken bezüglich der Sammlung von Daten zu beachten. Wir wissen, dass Sie vielleicht Fragen dazu haben, in welcher Weise Kaspersky Security Network Daten und Informationen sammelt und nutzt, und wir haben diese Erklärung („Erklärung zur Datensammlung“ oder „Erklärung“) verfasst, um Sie über die Grundsätze der Sammlung von Daten zu informieren, nach denen Kaspersky Security Network vorgeht.

Diese Erklärung enthält etliche allgemeine und technische Einzelheiten über die Maßnahmen, die wir unternehmen, um Ihre Bedenken bezüglich der Sammlung von Daten auszuräumen. Wir haben diese Erklärung in verschiedene Bereiche aufgeteilt, so dass Sie schnell und einfach die Information finden, die Sie gerade benötigen. Der Hauptgedanke ist, dass Ihre Wünsche und Erwartungen die Grundlage für alles bilden, was wir tun – einschließlich des Schutzes Ihrer Daten.

Die Angaben und Informationen wurden von Kaspersky Lab zusammengestellt und wenn Sie nach dem Studium dieser Erklärung noch Fragen oder Bedenken zum Datenschutz haben, schicken Sie bitte eine e-mail an support@kaspersky.com.

Was ist Kaspersky Security Network?

Das Kaspersky Security Network ermöglicht es weltweit allen Nutzern von Kaspersky Lab- Sicherheitsprodukten, dabei zu helfen, die Identifikation von neuen („in the Wild“ auftretenden) Sicherheitsrisiken, die Ihren Computer bedrohen, zu erleichtern und die Zeit zu verkürzen, um einen Schutz dagegen zu entwickeln. Um neue Bedrohungen und ihre Ausgangspunkte zu identifizieren und um die Sicherheit der Nutzer und die Funktion der Produkte sicherzustellen, sammelt Kaspersky Security Network bestimmte Sicherheits- und Anwendungsdaten über mögliche Sicherheitsrisiken und übermittelt diese Angaben zur Analyse an Kaspersky Lab. Diese Informationen enthalten keinerlei Angaben, die den Anwender persönlich identifizierbar machen, und sie werden von Kaspersky Lab ausschließlich benutzt, um die Sicherheit ihrer Produkte zu erhöhen und zukünftige Lösungen gegen Schadsoftware und Viren zu finden. Falls es im Einzelfall dennoch zu ungewollten Übertragungen von persönlichen Daten eines Anwenders kommen sollte, wird Kaspersky Lab diese streng nach den Vorgaben dieser Erklärung behandeln und schützen.

Indem Sie am Kaspersky Security Network teilnehmen, tragen Sie und die anderen Nutzer der Kaspersky Lab-Sicherheitsprodukte erheblich zu einem sichereren Internet bei.

Rechtliche Aspekte

Kaspersky Security Network unterliegt den Gesetzen verschiedener Rechtssysteme, weil seine Dienste in Ländern mit unterschiedlicher Gesetzgebung genutzt werden, einschließlich der Vereinigten Staaten von Amerika. Kaspersky Lab wird persönliche Daten auch ohne Ihre Erlaubnis offen legen, wenn dies durch Gesetz gefordert wird, oder im Guten Glauben, dass ein solches Vorgehen erforderlich ist, um schädigendes Verhalten gegen Gäste, Besucher und Mitarbeiter von Kaspersky Lab, sein Eigentum oder andere Rechtsgüter zu verfolgen oder davor zu schützen. Wie erwähnt, können sich Gesetze, die die von Kaspersky Lab gesammelten Daten und Informationen betreffen, von Land zu Land unterscheiden. Zum Beispiel unterliegen einige der gesammelten Daten und Informationen in der Europäischen Union

und ihren Mitgliedstaaten den EU-Richtlinien über persönliche Daten, Privatsphäre und elektronische Kommunikation, einschließlich, aber nicht beschränkt auf die Richtlinie 2002/58/EC des Europäischen Parlamentes und des Ministerrates vom 12.07.2002 über die Behandlung von persönlichen Daten und den Schutz der Privatsphäre im Bereich der elektronischen Kommunikation und die Richtlinie 95/46/EC des Europäischen Parlamentes und des Ministerrates vom 24.10.1995 über den Schutz des Individuums unter Berücksichtigung der Verarbeitung von persönlichen Daten und über den freien Austausch solcher Daten und die daraus folgende Gesetzgebung in den Mitgliedstaaten der EU, sowie die Entscheidung der Europäischen Kommission Nr. 497/2001/EC über allgemeine Vertragsbedingungen (betreffend die Übermittlung von persönlichen Daten an Drittstaaten) und die daraus folgende Gesetzgebung in den Mitgliedstaaten der EU.

Kaspersky Security Network wird die betroffenen Anwender informieren, wenn die oben erwähnten Informationen erstmalig gesammelt werden, ob diese Informationen weitergegeben werden, insbesondere zu geschäftlichen Zwecken, und wird diesen Internetnutzern die Möglichkeit geben, online der geschäftlichen Nutzung und der Weitergabe an Dritte entweder ausdrücklich zuzustimmen („opt-in“, in den Mitgliedstaaten der EU und anderen Ländern, die ein „opt-in“ verlangen) oder zu verlangen, dies zu unterlassen („opt-out“, in allen anderen Ländern).

Kaspersky Lab kann möglicherweise durch Gesetz oder durch die Justizbehörden aufgefordert werden, gewisse persönliche identifizierbare Daten bestimmten staatlichen Behörden offenzulegen. Wenn dies durch Gesetz oder Justizbehörden gefordert wird, werden wir diese Informationen gegen entsprechende Bestätigung herausgeben. Kaspersky Lab kann außerdem Informationen gegenüber der Justiz offen legen, um sein Eigentum sowie die Gesundheit und die Sicherheit von Personen zu schützen, soweit dies gesetzlich erlaubt ist.

Angaben zu den für den Datenschutz zuständigen Behörden der Mitgliedstaaten werden entsprechend der jeweils aktuellen Gesetzgebung der EU-Mitgliedstaaten gemacht. Informationen zu diesen Angaben sind im Servicebereich von Kaspersky Security Network verfügbar.

B. GESAMMELTE INFORMATIONEN

Welche Daten wir sammeln

Der Benutzer besitzt das Recht, in Übereinstimmung mit dieser Erklärung Daten zur Verfügung zu stellen und der Kaspersky Security Network-Service sammelt grundlegende und weitergehende Daten über mögliche Sicherheitsrisiken, die Ihren Computer bedrohen, und gibt diese an Kaspersky Lab weiter. Die gesammelten Daten umfassen:

Grundlegende Daten:

- Informationen über Ihre Hardware und Software, einschließlich Betriebssystem und installierte Service-Packs, Kernel-Objekte, Treiber, Dienstprogramme, Internet Explorer-Erweiterungen, Druckerweiterungen, Windows Explorer-Erweiterungen, heruntergeladene Programme, aktive Setup-Elemente, Ergänzungen der Taskleiste, Host- und Registry-Aufzeichnungen, IP-Adressen, Browsertyp, e-mail clients und die Versionsnummer des Kaspersky Lab-Produktes, diese lässt grundsätzlich keine persönliche Identifizierung zu.

- Eine individuelle ID, die vom Kaspersky Lab-Produkt zur Identifizierung bestimmter Maschinen erzeugt wird, ohne den Anwender zu identifizieren, und die keinerlei persönliche Informationen enthält.

- Informationen über den Stand des Schutzes vor Viren und Daten über alle Dateien oder Aktivitäten, die im Verdacht stehen, Malware zu sein (z.B. Virenname, Datum und Zeit der Entdeckung, Namen, Pfade und Größe der infizierten Dateien, IP und den Port einer Netzwerk-Attacke, Name der Anwendung, die im Verdacht steht, Malware zu sein). Bitte nehmen Sie zur Kenntnis, dass die erwähnten Daten keinerlei persönliche identifizierbare Informationen enthalten.

Weitergehende Daten:

- Informationen über vom Nutzer heruntergeladene digital signierte Anwendungen (URL, Dateigröße, Name des Signierenden)

- Informationen über ausführbare Anwendungen (Größe, Attribute, Erstellungsdatum, Informationen zum PE-Header, Regionalcode, Name, Herkunft und benutzte Kompressionsmethode)

Dateien und/oder deren Teile

Der Dienst Kaspersky Security Network kann ganze Dateien und/oder deren Teile sammeln und zum Zweck einer zusätzlichen Analyse an Kaspersky Lab übermitteln. Die Übermittlung von Dateien und/oder deren Teilen erfolgt nur, wenn Sie die Erklärung zur Datensammlung von Kaspersky Lab akzeptiert haben.

Sichern der Übertragung und der Aufbewahrung von Daten

Kaspersky Lab verpflichtet sich, die Sicherheit der gesammelten Informationen zu schützen. Die gesammelten Informationen werden auf Computer-Servern mit eingeschränktem und kontrolliertem Zugang gespeichert. Kaspersky Lab betreibt sichere Datennetzwerke, die durch Firewalls nach Industriestandard und durch passwortgeschützte Systeme geschützt sind. Kaspersky Lab nutzt umfangreiche Sicherheitstechnologien und Prozesse, um die gesammelten Informationen vor Bedrohungen durch unberechtigten Zugriff, Nutzung oder Offenlegung zu schützen. Unsere Sicherheitsrichtlinien werden regelmäßig überprüft und wenn nötig ergänzt, ausschließlich berechtigte Personen haben auf die gesammelten Daten Zugriff. Kaspersky Lab sorgt dafür, dass Ihre Informationen sicher und in Übereinstimmung mit dieser Erklärung behandelt werden. Bedauerlicherweise kann jedoch für keine Datenübertragung Sicherheit absolut garantiert werden. Daher können wir bei allem Bemühen, Ihre Daten zu schützen, nicht die Sicherheit aller Daten garantieren, die von Ihnen, unseren Produkten oder Diensten an uns übertragen werden, einschließlich, aber nicht darauf beschränkt, des Kaspersky Security Network. Sie nutzen alle diese Dienste auf Ihr eigenes Risiko.

Die gesammelten Daten werden an die Server von Kaspersky Lab übertragen und Kaspersky Lab hat die nötigen Vorsichtsmaßnahmen getroffen, um sicherzustellen, dass die gesammelten Informationen, wenn sie übertragen sind, auf einem angemessenen Niveau geschützt sind. Wir behandeln die von uns gesammelten Daten als vertraulich, sie unterliegen demzufolge unseren Sicherheitsmaßnahmen und unseren Richtlinien bezüglich des Schutzes und des Gebrauchs von vertraulichen Informationen. Wenn die gesammelten Daten Kaspersky Lab erreichen, werden sie auf einem Server gespeichert, der mit branchenüblichen Sicherheitsmaßnahmen versehen ist, einschließlich Nutzung von Login/Passwort-Verfahren und elektronischen Firewalls, die einen unberechtigten Zugriff von außerhalb verhindern. Vom Kaspersky Security Network gesammelte und unter diese Erklärung fallende Daten werden in den USA und ggf. unter weiteren Rechtssystemen erhoben und gespeichert, ebenso in anderen Staaten, in denen Kaspersky Lab tätig ist. Alle Mitarbeiter von Kaspersky Lab beachten unsere Sicherheitsbestimmungen. Ihre Daten sind nur jenen Mitarbeitern zugänglich, die sie für ihre Arbeit benötigen. Keine gespeicherten Daten werden mit irgendeiner Information verbunden, die eine persönliche Identifikation ermöglicht. Kaspersky Lab vermischt die durch das Kaspersky Security Network gespeicherten Daten in keinem Fall mit Daten, Kontaktlisten oder vorgemerkten Informationen, die Kaspersky Lab für Werbung oder zu anderen Zwecken gesammelt hat.

C. VERWENDUNG DER GESAMMELTEN DATEN

Wie Ihre persönlichen Informationen verwendet werden

Kaspersky Lab sammelt die Daten, um die Quellen von potentiellen Sicherheitsrisiken zu analysieren und zu identifizieren und die Fähigkeit von Kaspersky Lab-Produkten zu verbessern, verdächtiges Verhalten im Internet, betrügerische Websites, Crimeware und andere Arten von Sicherheitsbedrohungen im Internet aufzuspüren, um so auch zukünftig den bestmöglichen Schutz für die Kunden von Kaspersky Lab sicherzustellen.

Offenlegung von Informationen gegenüber Dritten

Kaspersky Lab kann jede der gesammelten Informationen offen legen, wenn es von einer Justizbehörde gefordert und aufgrund eine Gesetzes erlaubt oder gefordert ist oder aufgrund einer Vorladung oder eines anderen Rechtsinstrumentes, oder wenn wir in Gutem Glauben annehmen, dergestalt handeln zu müssen, um anwendbares Recht zu erfüllen, oder um einer Vorladung, einem anderen Rechtsinstrument oder einer durchsetzbaren staatlichen Anforderung zu entsprechen. Kaspersky Lab kann weiterhin persönliche Informationen, die Identifikationen zulassen, offen legen, wenn Grund zu der Annahme besteht, dass die Offenlegung dieser Information notwendig ist, um jemanden zu identifizieren, seiner habhaft zu werden oder rechtliche Mittel gegen ihn zu ermöglichen, der diese Erklärung oder die Inhalte Ihrer Vereinbarung mit uns verletzt haben könnte, oder um die Sicherheit unserer Nutzer und der Öffentlichkeit zu schützen, oder unter Beachtung von Geheimhaltungs- und Lizenzbestimmungen gegenüber Dritten, die uns bei Entwicklung, Betrieb und Wartung des Kaspersky Security Network unterstützen. Um die allgemeine Aufmerksamkeit sowie die Entdeckung von und die Vorbeugung vor Sicherheitsrisiken im Internet zu fördern, darf Kaspersky Lab bestimmte Informationen mit Forschungseinrichtungen und anderen Softwareanbietern teilen. Kaspersky Lab darf darüber hinaus Statistiken verwenden, die aus den gesammelten Informationen erstellt wurden, um Berichte über Entwicklungen von Sicherheitsrisiken zu erstellen und zu veröffentlichen.

Ihre Wahlmöglichkeiten

Die Teilnahme am Kaspersky Security Network ist optional. Sie können das Kaspersky Security Network jederzeit aktivieren bzw. deaktivieren, indem Sie die Feedback-Einstellungen unter den „Optionen“ Ihres Kaspersky-Produktes aufsuchen. Bitte beachten Sie jedoch, wenn Sie sich entschließen, den Kaspersky Security Network-Service zu deaktivieren, dass wir Sie in diesem Fall nicht mit einigen Leistungen versorgen können, die von der Sammlung dieser Daten abhängig sind.

Wenn die Wartungsperiode Ihres Kaspersky Lab-Produktes abläuft, kann es sein, dass einige Funktionen der Software weiterhin zur Verfügung stehen, aber es werden keine Informationen mehr automatisch an Kaspersky Lab gesendet.

Wir behalten aus außerdem das Recht vor, unregelmäßige Alarmmeldungen an die Nutzer zu senden, um sie über spezifische Änderungen zu informieren, die ihre Fähigkeit zur Nutzung unserer Dienste, für die sie sich entschieden

haben, beeinflussen können. Wir behalten uns weiterhin das Recht vor, Sie zu kontaktieren, wenn es aus rechtlichen Gründen notwendig ist oder wenn eine Verletzung einer gültigen Lizenz, Garantie oder Verkaufsbestimmung vorliegt.

Kaspersky Lab behält sich diese Rechte vor, weil wir in einzelnen Fällen der Meinung sind, das Recht zu benötigen, mit Ihnen in Kontakt zu treten, sei es aus rechtlichen Gründen oder aus sonstigen Gründen, die für Sie wichtig sein können. Diese Rechte erlauben uns jedoch nicht, Sie anzusprechen, um neue oder auch bestehende Dienstleistungen zu bewerben, wenn Sie uns dies nicht gestattet haben, und die Anlässe für diese Arten der Kommunikation sind in der Praxis selten.

D. DATENSAMMLUNG – WEITERE FRAGEN UND BESCHWERDEN

Kaspersky Lab behandelt die Bedenken seiner Nutzer bezüglich der Datensammlung mit äußerstem Respekt und Aufmerksamkeit. Wenn Sie mit einem Punkt dieser Erklärung in Bezug auf Ihre Informationen oder Daten nicht einverstanden sind oder wenn Sie andere Fragen oder Beschwerden haben, schreiben Sie uns oder kontaktieren Sie Kaspersky Lab per e-mail: support@kaspersky.com.

Beschreiben Sie in Ihrer Nachricht bitte so genau wie möglich den Grund Ihrer Nachfrage. Wir werden Ihrer Frage oder Beschwerde unverzüglich nachgehen.

Die Bereitstellung von Informationen ist freiwillig. Die Option der Datensammlung kann vom Anwender jederzeit im Bereich „Feedback“ auf der Seite „Einstellungen“ des entsprechenden Kaspersky-Produktes abgeschaltet werden.

Copyright © Kaspersky Lab. Alle Rechte vorbehalten.

VERWENDUNG DES CODES VON DRITTHERSTELLERN

Bei der Entwicklung von Kaspersky Internet Security wurde der Code von Drittherstellern verwendet.

IN DIESEM ABSCHNITT

CryptoEx Ltd. 240

Bibliothek fastscript 1.9 240

Bibliothek pcre 7.4, 7.7 240

Bibliothek GNU bison parser 241

Bibliothek AGG 2.4 241

Bibliothek OpenSSL 0.9.8d 241

Bibliothek Gecko SDK 1.8 243

Bibliothek zlib 1.2 243

Bibliothek libpng 01.02.08, 01.02.029 243

Bibliothek libnkfm 2.0.5 243

Bibliothek expat 1.2, 2.0.1 243

Bibliothek Info-ZIP 5.51 244

Bibliothek Windows Installer XML (WiX) 2.0 244

Bibliothek passthru 247

Bibliothek filter 247

Bibliothek netcfg 247

Bibliothek pcre 3.0 247

Bibliothek RFC1321-based (RSA-free) MD5 library 248

Bibliothek Windows Template Library (WTL 7.5) 248

Bibliothek libjpeg 6b 251

Bilbiothek libungif 3.0 252

Bibliothek libxdr 252

Bibliothek tiniconv - 1.0.0 253

Bibliothek bzip2/libbzip2 1.0.5 257

Bibliothek libspf2-1.2.9 258

Bibliothek Protocol Buffer 258

CryptoEx Ltd.

Für die Erstellung und Überprüfung elektronischer digitaler Signaturen wird in Kaspersky Internet Security die Krypto-Bibliothek (Programmbibliothek zum Informationsschutz - PBSI) "Crypto-Si" verwendet, die von CryptoEx Ltd. entwickelt wurde. CryptoEx Ltd. verfügt über eine FAPSI-Lizenz (FSB) und über ein Zertifikat für die Krypto-Bibliothek "Crypto-Si".

Webseite von CryptoEx Ltd.: http://www.cryptoex.ru

Die Rechte an der Krypto-Bibliothek sind exklusives Eigentum der CryptoEx Ltd.

Bibliothek FastScript 1.9

Bei der Entwicklung des Programms wurde die Bibliothek FastScript copyright © Fast Reports Inc. verwendet. All rights reserved.

Bibliothek pcre 7.4, 7.7

Bei der Entwicklung des Programms wurde die Bibliothek pcre 7.4, 7.7 nach den Nutzungsbedingungen der Lizenz BSD verwendet. Copyright © 1997-2008 University of Cambridge.

PCRE is a library of functions to support regular expressions whose syntax and semantics are as close as possible to those of the Perl 5 language.

Release 5 of PCRE is distributed under the terms of the "BSD" licence, as specified below. The documentation for PCRE, supplied in the "doc" directory, is distributed under the same terms as the software itself.

Written by: Philip Hazel <ph10@cam.ac.uk>

University of Cambridge Computing Service,

Cambridge, England. Phone: +44 1223 334714.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- Neither the name of the University of Cambridge nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

BIBLIOTHEK GNU BISON PARSER

Bei der Entwicklung des Programms wurde die Bibliothek bison parser skeleton 2.3 copyright © GNU Project http://ftp.gnu.org/gnu/bison/ im Rahmen einer Sondergenehmigung verwendet.

As a special exception, you may create a larger work that containspart or all of the Bison parser skeleton and distribute that work under terms of your choice, so long as that work isn't itself a parser generator using the skeleton or a modified version thereof as a parser skeleton. Alternatively, if you modify or redistribute the parser skeleton itself, you may (at your option) remove this special exception, which will cause the skeleton and the resulting Bison output files to be licensed under the GNU General Public License without this special exception.

BIBLIOTHEK AGG 2.4

Bei der Entwicklung des Programms wurde die Bibliothek AGG (Anti-Grain Geometry) 2.4 verwendet. Copyright © 2002-2005 Maxim Shemanarev. All rights reserved, mit modifizierter BSD-Lizenz.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Copyright (c) 2004 Alberto Demichelis

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.

2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.

3. This notice may not be removed or altered from any source distribution.

BIBLIOTHEK OPENSSL 0.9.8D

Bei der Entwicklung des Programms wurde die Bibliothek OpenSSL 0.9.8d verwendet. Copyright © 1998-2007 The OpenSSL Project. All rights reserved, mit der Lizenz von OpenSSL License und der Original SSLeay License (http://www.openssl.org/).

OpenSSL License

Copyright (c) 1998-2007 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)"

4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com) All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are aheared to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com). Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement:"This product includes cryptographic software written byEric Young (eay@cryptsoft.com)" The word 'cryptographic' can be left out if the rouines from the library being used are not cryptographic related).

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)".

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]

BIBLIOTHEK GECKO SDK 1.8

Bei der Entwicklung des Programms wurde die Bibliothek Gecko SDK 1.8 verwendet. Copyright © Mozilla Foundation. All rights reserved, unter der Lizenz MPL 1.1 (http://www.mozilla.org/MPL/MPL-1.1.html). Webseite und Link zu der Distribution: http://developer.mozilla.org/en/docs/Gecko_SDK.

BIBLIOTHEK ZLIB 1.2

Bei der Entwicklung des Programms wurde die Bibliothek zlib 1.2 verwendet. Copyright © 1995-2005 Jean-loup Gailly and Mark Adler. Alle Rechte vorbehalten, nach den Nutzungsbedingungen der Lizenz zlib/libpng.

BIBLIOTHEK LIBPNG 01.02.08, 01.02.029

Bei der Entwicklung des Programms wurde die Bibliothek libpng 01.02.08, 01.02.29 verwendet. Copyright © 2004, 2006-2008 Glenn Randers-Pehrson. Alle Rechte vorbehalten, nach den Nutzungsbedingungen der Lizenz zlib/libpng.

BIBLIOTHEK LIBNKFM 2.0.5

Bei der Entwicklung des Programms wurde die Bibliothek libnkfm 2.0.5 verwendet. Copyright (c) KUBO Takehiro. All rights reserved.

BIBLIOTHEK EXPAT 1.2, 2.0.1

Bei der Entwicklung des Programms wurde die Bibliothek Expat 1.2, 2.0.1 verwendet. Copyright (c) 1998, 1999, 2000 Thai Open Source Software Center Ltd. Alle Rechte vorbehalten, Verwendung nach folgenden Nutzungsbedingungen:

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

BIBLIOTHEK INFO-ZIP 5.51

Bei der Entwicklung des Programms wurde die Bibliothek Info-ZIP 5.51 verwendet. Copyright (c) 1990-2007. Alle Rechte vorbehalten, nach den Nutzungsbedingungen der Lizenz Info-ZIP.

This software is provided "as is," without warranty of any kind, express or implied. In no event shall Info-ZIP or its contributors be held liable for any direct, indirect, incidental, special or consequential damages arising out of the use of or inability to use this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the above disclaimer and the following restrictions:

1. Redistributions of source code (in whole or in part) must retain the above copyright notice, definition, disclaimer, and this list of conditions.

2. Redistributions in binary form (compiled executables and libraries) must reproduce the above copyright notice, definition, disclaimer, and this list of conditions in documentation and/or other materials provided with the distribution. The sole exception to this condition is redistribution of a standard UnZipSFX binary (including SFXWiz) as part of a self-extracting archive; that is permitted without inclusion of this license, as long as the normal SFX banner has not been removed from the binary or disabled.

3. Altered versions--including, but not limited to, ports to new operating systems, existing ports with new graphical interfaces, versions with modified or added functionality, and dynamic, shared, or static library versions not from Info-ZIP--must be plainly marked as such and must not be misrepresented as being the original source or, if binaries, compiled from the original source. Such altered versions also must not be misrepresented as being Info-ZIP releases--including, but not limited to, labeling of the altered versions with the names "Info-ZIP" (or any variation thereof, including, but not limited to, different capitalizations), "Pocket UnZip," "WiZ" or "MacZip" without the explicit permission of Info-ZIP. Such altered versions are further prohibited from misrepresentative use of the Zip-Bugs or Info-ZIP e-mail addresses or the Info-ZIP URL(s), such as to imply Info-ZIP will provide support for the altered versions.

4. Info-ZIP retains the right to use the names "Info-ZIP," "Zip," "UnZip, "UnZipSFX," "WiZ," "Pocket UnZip," "Pocket Zip," and "MacZip" for its own source and binary releases.

BIBLIOTHEK WINDOWS INSTALLER XML (WIX) 2.0

Bei der Entwicklung des Programms wurde die Bibliothek Windows Installer XML (WiX) 2.0 verwendet. Copyright (c) Microsoft Corporation. All rights reserved, unter der Lizenz CPL 1.0 (http://sourceforge.net/projects/wix/).

Common Public License Version 1,0

THE ACCOMPANYING PROGRAM IS PROVIDED UNDER THE TERMS OF THIS COMMON PUBLIC LICENSE ("AGREEMENT"). ANY USE, REPRODUCTION OR DISTRIBUTION OF THE PROGRAM CONSTITUTES RECIPIENT'S ACCEPTANCE OF THIS AGREEMENT.

1. **DEFINITIONS**

   "Contribution" means:

   a) in the case of the initial Contributor, the initial code and documentation distributed under this Agreement, and

b) in the case of each subsequent Contributor:

i) changes to the Program, and

ii) additions to the Program;

where such changes and/or additions to the Program originate from and are distributed by that particular Contributor. A Contribution 'originates' from a Contributor if it was added to the Program by such Contributor itself or anyone acting on such Contributor's behalf. Contributions do not include additions to the Program which: (i) are separate modules of software distributed in conjunction with the Program under their own license agreement, and (ii) are not derivative works of the Program.

"Contributor" means any person or entity that distributes the Program.

"Licensed Patents " mean patent claims licensable by a Contributor which are necessarily infringed by the use or sale of its Contribution alone or when combined with the Program.

"Program" means the Contributions distributed in accordance with this Agreement.

"Recipient" means anyone who receives the Program under this Agreement, including all Contributors.

2. **GRANT OF RIGHTS**

a) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free copyright license to reproduce, prepare derivative works of, publicly display, publicly perform, distribute and sublicense the Contribution of such Contributor, if any, and such derivative works, in source code and object code form.

b) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free patent license under Licensed Patents to make, use, sell, offer to sell, import and otherwise transfer the Contribution of such Contributor, if any, in source code and object code form. This patent license shall apply to the combination of the Contribution and the Program if, at the time the Contribution is added by the Contributor, such addition of the Contribution causes such combination to be covered by the Licensed Patents. The patent license shall not apply to any other combinations which include the Contribution. No hardware per se is licensed hereunder.

c) Recipient understands that although each Contributor grants the licenses to its Contributions set forth herein, no assurances are provided by any Contributor that the Program does not infringe the patent or other intellectual property rights of any other entity. Each Contributor disclaims any liability to Recipient for claims brought by any other entity based on infringement of intellectual property rights or otherwise. As a condition to exercising the rights and licenses granted hereunder, each Recipient hereby assumes sole responsibility to secure any other intellectual property rights needed, if any. For example, if a third party patent license is required to allow Recipient to distribute the Program, it is Recipient's responsibility to acquire that license before distributing the Program.

d) Each Contributor represents that to its knowledge it has sufficient copyright rights in its Contribution, if any, to grant the copyright license set forth in this Agreement.

3. **REQUIREMENTS**

A Contributor may choose to distribute the Program in object code form under its own license agreement, provided that:

a) it complies with the terms and conditions of this Agreement; and

b) its license agreement:

i) effectively disclaims on behalf of all Contributors all warranties and conditions, express and implied, including warranties or conditions of title and non-infringement, and implied warranties or conditions of merchantability and fitness for a particular purpose;

ii) effectively excludes on behalf of all Contributors all liability for damages, including direct, indirect, special, incidental and consequential damages, such as lost profits;

iii) states that any provisions which differ from this Agreement are offered by that Contributor alone and not by any other party; and

iv) states that source code for the Program is available from such Contributor, and informs licensees how to obtain it in a reasonable manner on or through a medium customarily used for software exchange.

When the Program is made available in source code form:

a) it must be made available under this Agreement; and

b) a copy of this Agreement must be included with each copy of the Program.

Contributors may not remove or alter any copyright notices contained within the Program.

Each Contributor must identify itself as the originator of its Contribution, if any, in a manner that reasonably allows subsequent Recipients to identify the originator of the Contribution.

4. **COMMERCIAL DISTRIBUTION**

Commercial distributors of software may accept certain responsibilities with respect to end users, business partners and the like. While this license is intended to facilitate the commercial use of the Program, the Contributor who includes the Program in a commercial product offering should do so in a manner which does not create potential liability for other Contributors. Therefore, if a Contributor includes the Program in a commercial product offering, such Contributor ("Commercial Contributor") hereby agrees to defend and indemnify every other Contributor ("Indemnified Contributor") against any losses, damages and costs (collectively "Losses") arising from claims, lawsuits and other legal actions brought by a third party against the Indemnified Contributor to the extent caused by the acts or omissions of such Commercial Contributor in connection with its distribution of the Program in a commercial product offering. The obligations in this section do not apply to any claims or Losses relating to any actual or alleged intellectual property infringement. In order to qualify, an Indemnified Contributor must: a) promptly notify the Commercial Contributor in writing of such claim, and b) allow the Commercial Contributor to control, and cooperate with the Commercial Contributor in, the defense and any related settlement negotiations. The Indemnified Contributor may participate in any such claim at its own expense.

For example, a Contributor might include the Program in a commercial product offering, Product X. That Contributor is then a Commercial Contributor. If that Commercial Contributor then makes performance claims, or offers warranties related to Product X, those performance claims and warranties are such Commercial Contributor's responsibility alone. Under this section, the Commercial Contributor would have to defend claims against the other Contributors related to those performance claims and warranties, and if a court requires any other Contributor to pay any damages as a result, the Commercial Contributor must pay those damages.

5. **NO WARRANTY**

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, THE PROGRAM IS PROVIDED ON AN "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, EITHER EXPRESS OR IMPLIED INCLUDING, WITHOUT LIMITATION, ANY WARRANTIES OR CONDITIONS OF TITLE, NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Each Recipient is solely responsible for determining the appropriateness of using and distributing the Program and assumes all risks associated with its exercise of rights under this Agreement, including but not limited to the risks and costs of program errors, compliance with applicable laws, damage to or loss of data, programs or equipment, and unavailability or interruption of operations.

6. **DISCLAIMER OF LIABILITY**

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, NEITHER RECIPIENT NOR ANY CONTRIBUTORS SHALL HAVE ANY LIABILITY FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING WITHOUT LIMITATION LOST PROFITS), HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OR DISTRIBUTION OF THE PROGRAM OR THE EXERCISE OF ANY RIGHTS GRANTED HEREUNDER, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

7. **GENERAL**

If any provision of this Agreement is invalid or unenforceable under applicable law, it shall not affect the validity or enforceability of the remainder of the terms of this Agreement, and without further action by the parties hereto, such provision shall be reformed to the minimum extent necessary to make such provision valid and enforceable.

If Recipient institutes patent litigation against a Contributor with respect to a patent applicable to software (including a cross-claim or counterclaim in a lawsuit), then any patent licenses granted by that Contributor to such Recipient under this Agreement shall terminate as of the date such litigation is filed. In addition, if Recipient institutes patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Program itself (excluding combinations of the Program with other software or hardware) infringes such Recipient's patent(s), then such Recipient's rights granted under Section 2(b) shall terminate as of the date such litigation is filed.

All Recipient's rights under this Agreement shall terminate if it fails to comply with any of the material terms or conditions of this Agreement and does not cure such failure in a reasonable period of time after becoming aware of such noncompliance. If all Recipient's rights under this Agreement terminate, Recipient agrees to cease use and distribution of the Program as soon as reasonably practicable. However, Recipient's obligations under this Agreement and any licenses granted by Recipient relating to the Program shall continue and survive.

Everyone is permitted to copy and distribute copies of this Agreement, but in order to avoid inconsistency the Agreement is copyrighted and may only be modified in the following manner. The Agreement Steward reserves the right to publish new versions (including revisions) of this Agreement from time to time. No one other than the Agreement Steward has the right to modify this Agreement. IBM is the initial Agreement Steward. IBM may assign the responsibility to serve as the Agreement Steward to a suitable separate entity. Each new version of the Agreement will be given a distinguishing version number. The Program (including Contributions) may always be distributed subject to the version of the Agreement under which it was received. In addition, after a new version of the Agreement is published, Contributor may elect to distribute the Program (including its Contributions) under the new version. Except as expressly stated in Sections 2(a) and 2(b) above, Recipient receives no rights or licenses to the intellectual property of any Contributor under this Agreement, whether expressly, by implication, estoppel or otherwise. All rights in the Program not expressly granted under this Agreement are reserved.

This Agreement is governed by the laws of the State of New York and the intellectual property laws of the United States of America. No party to this Agreement will bring a legal action under this Agreement more than one year after the cause of action arose. Each party waives its rights to a jury trial in any resulting litigation.

BIBLIOTHEK PASSTHRU

Bei der Entwicklung des Programms wurde die Biliothek Ndis Intermediate Miniport driver sample Copyright (c) 1992-2000 Microsoft Corporation verwendet. All rights reserved.

BIBLIOTHEK FILTER

Bei der Entwicklung des Programms wurde die Bibliothek Bibliothek Ndis Sample NDIS Lightweight filter driver verwendet. Copyright (c) 2004-2005 Microsoft Corporation. All rights reserved.

BIBLIOTHEK NETCFG

Bei der Entwicklung des Programms wurde die Bibliothek Network Configuration Sample Copyright (c) 1997 Microsoft Corporation verwendet. All rights reserved.

BIBLIOTHEK PCRE 3.0

Bei der Entwicklung des Programms wurde die Bibliothek pcre 3.0 nach den Nutzungsbedingungen der Lizenz PCRE LICENCE verwendet. Copyright © 1997-1999 University of Cambridge. All rights reserved.

BIBLIOTHEK RFC1321-BASED (RSA-FREE) MD5 LIBRARY

Bei der Entwicklung des Programms wurde die Bibliothek – RFC1321-based (RSA-free) MD5 library verwendet. Copyright (c) 1999, 2002 Aladdin Enterprises. All rights reserved. Sie wird verbreitet unter der Lizenz zlib/libpng.

BIBLIOTHEK WINDOWS TEMPLATE LIBRARY (WTL 7.5)

Bei der Entwicklung des Programms wurde die Bibliothek Windows Template Library 7.5 verwendet. Copyright (c) 2005 Microsoft Corporation. All rights reserved, unter der Lizenz Common Public license 1.0, http://sourceforge.net/projects/wtl/.

Common Public License Version 1,0

THE ACCOMPANYING PROGRAM IS PROVIDED UNDER THE TERMS OF THIS COMMON PUBLIC LICENSE ("AGREEMENT"). ANY USE, REPRODUCTION OR DISTRIBUTION OF THE PROGRAM CONSTITUTES RECIPIENT'S ACCEPTANCE OF THIS AGREEMENT.

1. **DEFINITIONS**

   "Contribution" means:

   a) in the case of the initial Contributor, the initial code and documentation distributed under this Agreement, and

   b) in the case of each subsequent Contributor:

   i) changes to the Program, and

   ii) additions to the Program;

   where such changes and/or additions to the Program originate from and are distributed by that particular Contributor. A Contribution 'originates' from a Contributor if it was added to the Program by such Contributor itself or anyone acting on such Contributor's behalf. Contributions do not include additions to the Program which: (i) are separate modules of software distributed in conjunction with the Program under their own license agreement, and (ii) are not derivative works of the Program.

   "Contributor" means any person or entity that distributes the Program.

   "Licensed Patents " mean patent claims licensable by a Contributor which are necessarily infringed by the use or sale of its Contribution alone or when combined with the Program.

   "Program" means the Contributions distributed in accordance with this Agreement.

   "Recipient" means anyone who receives the Program under this Agreement, including all Contributors.

2. **GRANT OF RIGHTS**

   a) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free copyright license to reproduce, prepare derivative works of, publicly display, publicly perform, distribute and sublicense the Contribution of such Contributor, if any, and such derivative works, in source code and object code form.

   b) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free patent license under Licensed Patents to make, use, sell, offer to sell, import and otherwise transfer the Contribution of such Contributor, if any, in source code and object code form. This patent license shall apply to the combination of the Contribution and the Program if, at the time the Contribution is added by the Contributor, such addition of the Contribution causes such combination to be covered by the Licensed Patents. The patent license shall not apply to any other combinations which include the Contribution. No hardware per se is licensed hereunder.

c) Recipient understands that although each Contributor grants the licenses to its Contributions set forth herein, no assurances are provided by any Contributor that the Program does not infringe the patent or other intellectual property rights of any other entity. Each Contributor disclaims any liability to Recipient for claims brought by any other entity based on infringement of intellectual property rights or otherwise. As a condition to exercising the rights and licenses granted hereunder, each Recipient hereby assumes sole responsibility to secure any other intellectual property rights needed, if any. For example, if a third party patent license is required to allow Recipient to distribute the Program, it is Recipient's responsibility to acquire that license before distributing the Program.

d) Each Contributor represents that to its knowledge it has sufficient copyright rights in its Contribution, if any, to grant the copyright license set forth in this Agreement.

3. **REQUIREMENTS**

A Contributor may choose to distribute the Program in object code form under its own license agreement, provided that:

a) it complies with the terms and conditions of this Agreement; and

b) its license agreement:

i) effectively disclaims on behalf of all Contributors all warranties and conditions, express and implied, including warranties or conditions of title and non-infringement, and implied warranties or conditions of merchantability and fitness for a particular purpose;

ii) effectively excludes on behalf of all Contributors all liability for damages, including direct, indirect, special, incidental and consequential damages, such as lost profits;

iii) states that any provisions which differ from this Agreement are offered by that Contributor alone and not by any other party; and

iv) states that source code for the Program is available from such Contributor, and informs licensees how to obtain it in a reasonable manner on or through a medium customarily used for software exchange.

When the Program is made available in source code form:

a) it must be made available under this Agreement; and

b) a copy of this Agreement must be included with each copy of the Program.

Contributors may not remove or alter any copyright notices contained within the Program.

Each Contributor must identify itself as the originator of its Contribution, if any, in a manner that reasonably allows subsequent Recipients to identify the originator of the Contribution.

4. **COMMERCIAL DISTRIBUTION**

Commercial distributors of software may accept certain responsibilities with respect to end users, business partners and the like. While this license is intended to facilitate the commercial use of the Program, the Contributor who includes the Program in a commercial product offering should do so in a manner which does not create potential liability for other Contributors. Therefore, if a Contributor includes the Program in a commercial product offering, such Contributor ("Commercial Contributor") hereby agrees to defend and indemnify every other Contributor ("Indemnified Contributor") against any losses, damages and costs (collectively "Losses") arising from claims, lawsuits and other legal actions brought by a third party against the Indemnified Contributor to the extent caused by the acts or omissions of such Commercial Contributor in connection with its distribution of the Program in a commercial product offering. The obligations in this section do not apply to any claims or Losses relating to any actual or alleged intellectual property infringement. In order to qualify, an Indemnified Contributor must: a) promptly notify the Commercial Contributor in writing of such claim, and b) allow the Commercial Contributor to control, and cooperate with the Commercial Contributor in, the defense and any related settlement negotiations. The Indemnified Contributor may participate in any such claim at its own expense.

For example, a Contributor might include the Program in a commercial product offering, Product X. That Contributor is then a Commercial Contributor. If that Commercial Contributor then makes performance claims, or offers warranties related to Product X, those performance claims and warranties are such Commercial

Contributor's responsibility alone. Under this section, the Commercial Contributor would have to defend claims against the other Contributors related to those performance claims and warranties, and if a court requires any other Contributor to pay any damages as a result, the Commercial Contributor must pay those damages.

5. **NO WARRANTY**

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, THE PROGRAM IS PROVIDED ON AN "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, EITHER EXPRESS OR IMPLIED INCLUDING, WITHOUT LIMITATION, ANY WARRANTIES OR CONDITIONS OF TITLE, NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Each Recipient is solely responsible for determining the appropriateness of using and distributing the Program and assumes all risks associated with its exercise of rights under this Agreement, including but not limited to the risks and costs of program errors, compliance with applicable laws, damage to or loss of data, programs or equipment, and unavailability or interruption of operations.

6. **DISCLAIMER OF LIABILITY**

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, NEITHER RECIPIENT NOR ANY CONTRIBUTORS SHALL HAVE ANY LIABILITY FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING WITHOUT LIMITATION LOST PROFITS), HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OR DISTRIBUTION OF THE PROGRAM OR THE EXERCISE OF ANY RIGHTS GRANTED HEREUNDER, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

7. **GENERAL**

If any provision of this Agreement is invalid or unenforceable under applicable law, it shall not affect the validity or enforceability of the remainder of the terms of this Agreement, and without further action by the parties hereto, such provision shall be reformed to the minimum extent necessary to make such provision valid and enforceable.

If Recipient institutes patent litigation against a Contributor with respect to a patent applicable to software (including a cross-claim or counterclaim in a lawsuit), then any patent licenses granted by that Contributor to such Recipient under this Agreement shall terminate as of the date such litigation is filed. In addition, if Recipient institutes patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Program itself (excluding combinations of the Program with other software or hardware) infringes such Recipient's patent(s), then such Recipient's rights granted under Section 2(b) shall terminate as of the date such litigation is filed.

All Recipient's rights under this Agreement shall terminate if it fails to comply with any of the material terms or conditions of this Agreement and does not cure such failure in a reasonable period of time after becoming aware of such noncompliance. If all Recipient's rights under this Agreement terminate, Recipient agrees to cease use and distribution of the Program as soon as reasonably practicable. However, Recipient's obligations under this Agreement and any licenses granted by Recipient relating to the Program shall continue and survive.

Everyone is permitted to copy and distribute copies of this Agreement, but in order to avoid inconsistency the Agreement is copyrighted and may only be modified in the following manner. The Agreement Steward reserves the right to publish new versions (including revisions) of this Agreement from time to time. No one other than the Agreement Steward has the right to modify this Agreement. IBM is the initial Agreement Steward. IBM may assign the responsibility to serve as the Agreement Steward to a suitable separate entity. Each new version of the Agreement will be given a distinguishing version number. The Program (including Contributions) may always be distributed subject to the version of the Agreement under which it was received. In addition, after a new version of the Agreement is published, Contributor may elect to distribute the Program (including its Contributions) under the new version. Except as expressly stated in Sections 2(a) and 2(b) above, Recipient receives no rights or licenses to the intellectual property of any Contributor under this Agreement, whether expressly, by implication, estoppel or otherwise. All rights in the Program not expressly granted under this Agreement are reserved.

This Agreement is governed by the laws of the State of New York and the intellectual property laws of the United States of America. No party to this Agreement will bring a legal action under this Agreement more than one year after the cause of action arose. Each party waives its rights to a jury trial in any resulting litigation.

BIBLIOTHEK LIBJPEG 6B

Bei der Entwicklung des Programms wurde die Bibliothek libjpeg 6b verwendet. Copyright (c) 1991-1998, Thomas G. Lane. All Rights. Verwendung nach folgenden Nutzungsbedingungen:

LEGAL ISSUES

In plain English:

We don't promise that this software works. (But if you find any bugs, please let us know!)

You can use this software for whatever you want. You don't have to pay us.

You may not pretend that you wrote this software. If you use it in a program, you must acknowledge somewhere in your documentation that you've used the IJG code.

In legalese:

The authors make NO WARRANTY or representation, either express or implied, with respect to this software, its quality, accuracy, merchantability, or fitness for a particular purpose. This software is provided "AS IS", and you, its user, assume the entire risk as to its quality and accuracy.

Permission is hereby granted to use, copy, modify, and distribute this software (or portions thereof) for any purpose, without fee, subject to these conditions:

(1) If any part of the source code for this software is distributed, then this README file must be included, with this copyright and no-warranty notice unaltered; and any additions, deletions, or changes to the original files must be clearly indicated in accompanying documentation.

(2) If only executable code is distributed, then the accompanying documentation must state that "this software is based in part on the work of the Independent JPEG Group".

(3) Permission for use of this software is granted only if the user accepts full responsibility for any undesirable consequences; the authors accept NO LIABILITY for damages of any kind.

These conditions apply to any software derived from or based on the IJG code, not just to the unmodified library. If you use our work, you ought to acknowledge us.

Permission is NOT granted for the use of any IJG author's name or company name in advertising or publicity relating to this software or products derived from it. This software may be referred to only as "the Independent JPEG Group's software".

We specifically permit and encourage the use of this software as the basis of commercial products, provided that all warranty or liability claims are assumed by the product vendor.

ansi2knr.c is included in this distribution by permission of L. Peter Deutsch, sole proprietor of its copyright holder, Aladdin Enterprises of Menlo Park, CA. ansi2knr.c is NOT covered by the above copyright and conditions, but instead by the usual distribution terms of the Free Software Foundation; principally, that you must include source code if you redistribute it. (See the file ansi2knr.c for full details.) However, since ansi2knr.c is not needed as part of any program generated from the IJG code, this does not limit you more than the foregoing paragraphs do.

The Unix configuration script "configure" was produced with GNU Autoconf. It is copyright by the Free Software Foundation but is freely distributable. The same holds for its supporting scripts (config.guess, config.sub, ltconfig, ltmain.sh). Another support script, install-sh, is copyright by M.I.T. but is also freely distributable.

It appears that the arithmetic coding option of the JPEG spec is covered by patents owned by IBM, AT&T, and Mitsubishi. Hence arithmetic coding cannot legally be used without obtaining one or more licenses. For this reason, support for arithmetic coding has been removed from the free JPEG software.

(Since arithmetic coding provides only a marginal gain over the unpatented Huffman mode, it is unlikely that very many implementations will support it.) So far as we are aware, there are no patent restrictions on the remaining

code.

The IJG distribution formerly included code to read and write GIF files. To avoid entanglement with the Unisys LZW patent, GIF reading support has been removed altogether, and the GIF writer has been simplified to produce "uncompressed GIFs". This technique does not use the LZW algorithm; the resulting GIF files are larger than usual, but are readable by all standard GIF decoders.

We are required to state that "The Graphics Interchange Format(c) is the Copyright property of CompuServe Incorporated. GIF(sm) is a Service Mark property of CompuServe Incorporated."

BILBIOTHEK LIBUNGIF 3.0

Bei der Entwicklung des Programms wurde die Bibliothek libungif 3.0 verwendet. Copyright (c) 1997 Eric S. Raymond. Verwendung nach folgenden Nutzungsbedingungen:

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

BIBLIOTHEK LIBXDR

Bei der Entwicklung des Programms wurde die Bibliothek libxdr verwendet. Copyright © Sun Microsystems, Inc. Verwendung nach folgenden Nutzungsbedingungen:

Sun RPC is a product of Sun Microsystems, Inc. and is provided for unrestricted use provided that this legend is included on all tape media and as a part of the software program in whole or part.

Users may copy or modify Sun RPC without charge, but are not authorized to license or distribute it to anyone else except as part of a product or program developed by the user.

SUN RPC IS PROVIDED AS IS WITH NO WARRANTIES OF ANY KIND INCLUDING THE WARRANTIES OF DESIGN, MERCHANTIBILITY AND FITNESS FOR A PARTICULAR PURPOSE, OR ARISING FROM A COURSE OF DEALING, USAGE OR TRADE PRACTICE.

Sun RPC is provided with no support and without any obligation on the part of Sun Microsystems, Inc. to assist in its use, correction, modification or enhancement.

SUN MICROSYSTEMS, INC. SHALL HAVE NO LIABILITY WITH RESPECT TO THE INFRINGEMENT OF COPYRIGHTS, TRADE SECRETS OR ANY PATENTS BY SUN RPC OR ANY PART THEREOF.

In no event will Sun Microsystems, Inc. be liable for any lost revenue or profits or other special, indirect and consequential damages, even if Sun has been advised of the possibility of such damages.

Sun Microsystems, Inc.

2550 Garcia Avenue

Mountain View, California 94043

BIBLIOTHEK TINICONV - 1.0.0

Bei der Entwicklung des Programms wurde die Bibliothek tiniconv – 1.0.0 Copyright (C) Free Software Foundation, Inc. author Roman Rybalko (http://sourceforge.net/projects/tiniconv/) unter der Lizenz GNU LGPL 2.1 (http://www.gnu.org/) verwendet.

GNU LESSER GENERAL PUBLIC LICENSE v.2,1

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more

frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) The modified work must itself be a software library.

b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6,)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

BIBLIOTHEK BZIP2/LIBBZIP2 1.0.5

Bei der Entwicklung des Programms wurde die Bibliothek bzip2/libbzip2 1.0.5 verwendet. Copyright (C) 1996-2007 Julian R Seward. All rights reserved. Verwendung nach folgenden Nutzungsbedingungen:

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyrightnotice, this list of conditions and the following disclaimer.

2. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.

3. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.

4. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Julian Seward, jseward@bzip.org

BIBLIOTHEK LIBSPF2-1.2.9

Bei der Entwicklung des Programms wurde die Bibliothek libspf2-1.2.9 verwendet. Copyright 2005 by Shevek and Wayne Schlitt, all rights reserved, Verwendung nach den Nutzungsbedingungen von The two-clause BSD license:

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

BIBLIOTHEK PROTOCOL BUFFER

Bei der Entwicklung des Programms wurde die Bibliothek Protocol Buffer verwendet. Copyright 2008, Google Inc. All rights reserved, Sie wird verbreitet nach den Nutzungsbedingungen von New BSD License

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

- Neither the name of Google Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Code generated by the Protocol Buffer compiler is owned by the owner of the input file used when generating it. This code is not standalone and requires a support library to be linked with it. This support library is itself covered by the above license.

GLOSSAR

Eine Liste der Masken und Webressourcen, deren Inhalt der Benutzer vertraut. Webseiten, die einem Element dieser Liste entsprechen, werden von der Kaspersky Lab Software nicht auf das Vorhandensein schädlicher Objekte untersucht.

2-Channel-Gateway

Computer mit zwei Netzwerkadaptern, die an verschiedene Netzwerke angeschlossen sind und Daten von einem Netzwerk an ein anderes Netzwerk übermitteln.

Aktive Lizenz

Lizenz, die momentan für die Arbeit des Kaspersky-Lab-Programms verwendet wird. Die Lizenz legt die Gültigkeitsdauer für den vollen Funktionsumfang sowie die Lizenzpolitik für das Programm fest. Im Programm kann nur ein Schlüssel den Status "aktiv" besitzen.

Alternative NTFS-Datenströme

Datenströme des NTFS-Dateisystems (ADS, alternate data streams), die für zusätzliche Attribute oder Datei-Informationen vorgesehen sind.

Jede Datei im NTFS-Dateisystem stellt eine Auswahl von Datenströmen (streams) dar. In einem Datenstrom befindet sich der Datei-Inhalt, den man sehen kann, wenn man die Datei öffnet, die übrigen (alternativen) Datenströme sind für Meta-Informationen vorgesehen und bieten zum Beispiel die Kompatibilität des NTFS-Systems mit anderen Systemen, wie mit dem alten Dateisystem von Macintosh - Hierarchical File System (HFS). Die Datenströme lassen sich erstellen, löschen, separat speichern, umbenennen und sogar als Prozess starten.

Alternative Datenströme können von Angreifern missbraucht werden, um Daten des Computers heimlich zu übertragen oder zu empfangen.

Anstössige E-Mail

Nachricht, die anstößige Ausdrücke enthält.

Archiv

Datei, die ein oder mehrere Objekte "enthält", die ihrerseits auch Archive sein können.

Aufgabe

Funktionen, die das Kaspersky-Lab-Programm ausführen kann und die als Aufgaben realisiert sind, Beispiele: **Echtzeitschutz für Dateien**, **Vollständige Untersuchung des Computers**, **Datenbank-Update**.

Aufgabeneinstellungen

Parameter für die Arbeit des Programms, die für jeden Aufgabentyp individuell sind.

Ausnahme

Eine Ausnahme ist ein Objekt, das von der Untersuchung durch das Kaspersky-Lab-Programm ausgeschlossen wird. Von der Untersuchung können Dateien eines bestimmten Formats, Dateien nach Maske, bestimmte Bereiche (beispielsweise ein Ordner oder Programm) sowie Programmprozesse oder Objekte nach einem Bedrohungstyp gemäß der Klassifikation der Viren-Enzyklopädie ausgeschlossen werden. Für jede Aufgabe können individuelle Ausnahmen festgelegt werden.

Autostart-Objekte

Auswahl von Programmen, die für den Start und die korrekte Funktion des auf Ihrem Computer installierten Betriebssystems und der vorhandenen Software erforderlich sind. Diese Objekte werden jedes Mal beim Hochfahren des Betriebssystems gestartet. Es gibt Viren, die speziell diese Objekte infizieren können. Dadurch kann beispielsweise das Hochfahren des Betriebssystems blockiert werden.

BACKUP

Spezieller Speicher für Sicherungskopien von Objekten, die vor einer Desinfektion oder vor dem Löschen angelegt werden.

BENACHRICHTIGUNGSVORLAGE

Vorlage, mit der bei der Untersuchung erkannte infizierte Objekte gemeldet werden. Eine Benachrichtigungsvorlage enthält mehrere Einstellungen, die die Reihenfolge der Benachrichtigung, die Verbreitungsart und den Meldungstext definieren.

BOOTVIRUS

Virus, der die Bootsektoren von Computerlaufwerken infiziert. Der Virus "zwingt" das System beim Hochfahren, nicht auf den eigentlichen Bootcode zuzugreifen, sondern auf den Viruscode, der dann die Kontrolle übernimmt.

DATEIMASKE

Platzhalter für den Namen und die Erweiterung einer Datei, der aus allgemeinen Zeichen besteht. Die zwei wichtigsten Zeichen, die in Dateimasken verwendet werden sind ***** und **?** (wobei ***** für eine beliebige Anzahl von Zeichen und **?** für ein beliebiges Einzelzeichen steht). Mit Hilfe dieser Zeichen kann jede beliebige Datei dargestellt werden. Beachten Sie, dass Name und Endung einer Datei stets durch einen Punkt getrennt werden.

DATENBANKEN

Datenbanken, die von den Kaspersky-Lab-Spezialisten gepflegt werden und eine genaue Beschreibung aller momentan existierenden Bedrohungen der Computersicherheit sowie Methoden zu ihrer Identifikation und Desinfektion enthalten. Die Datenbanken werden von Kaspersky Lab laufend aktualisiert, wenn neue Bedrohungen auftauchen. Um die Erkennungsqualität für Bedrohungen zu steigern, empfehlen wir, regelmäßig Updates für die Datenbanken von den Kaspersky-Lab-Updateservern herunterzuladen.

DATENBANK FÜR PHISHING-WEBADRESSEN

Eine Liste der Webressourcen, die von den Kaspersky-Lab-Spezialisten als Phishing-Adressen eingestuft wurden. Die Datenbank wird regelmäßig aktualisiert und gehört zum Lieferumfang des Kaspersky-Lab-Programms.

DATENBANK FÜR VERDÄCHTIGE WEBADRESSEN

Eine Liste der Webressourcen, deren Inhalt als potentiell gefährlich eingestuft werden kann. Die Liste ist von den Kaspersky-Lab-Spezialisten angelegt, wird regelmäßig aktualisiert und gehört zum Lieferumfang des Programms.

DATENBANK-UPDATE

Eine Funktion, die vom Kaspersky-Lab-Programm ausgeführt wird und die es erlaubt, den aktuellen Zustand des Schutzes aufrecht zu erhalten. Dabei werden die Datenbanken von den Kaspersky-Lab-Updateservern auf den Computer kopiert und automatisch von der Anwendung übernommen.

DESINFEKTION VON OBJEKTEN

Methode zur Bearbeitung von infizierten Objekten, bei der die Daten vollständig oder teilweise wiederhergestellt werden oder eine Entscheidung darüber getroffen wird, dass die Desinfektion von Objekten nicht möglich ist. Die Desinfektion von Objekten erfolgt auf Basis der Einträge in den Datenbänken. Bei der Desinfektion können Daten teilweise verloren gehen.

DESINFEKTION VON OBJEKTEN BEIM NEUSTART

Methode zur Verarbeitung von infizierten Objekten, die im Augenblick der Desinfektion von anderen Programmen verwendet werden. Dabei wird eine Kopie des infizierten Objekts angelegt. Beim folgenden Neustart wird die Kopie desinfiziert und das infizierte Originalobjekt wird durch die desinfizierte Kopie ersetzt.

DOMAIN NAME SERVICE (DNS)

Verbreitetes System zur Umformung von Hostnamen (Computer oder anderes Netzwerkgerät) in eine IP-Adresse. DNS funktioniert in TCP/IP-Netzwerken. Im Einzelfall kann DNS auch umgekehrte Anfragen und Definitionen von Hostnamen nach dessen IP (PTR-Eintrag) speichern und verarbeiten. Die Auflösung von DNS-Namen erfolgt gewöhnlich durch Netzwerkprogramme und nicht durch die Benutzer.

DRINGENDES UPDATE

Kritisches Update für die Module des Kaspersky-Lab-Programms.

ECHTZEITSCHUTZ

Funktionsmodus des Programms, in dem Objekte im Echtzeitmodus auf schädlichen Code untersucht werden.

Das Programm fängt jeden Versuch zum Öffnen, Schreiben und Ausführen eines Objekts ab, und durchsucht das Objekt nach Bedrohungen. Virenfreie Objekte werden für den Zugriff freigegeben, infizierte oder verdächtige Objekte werden gemäß den Aufgabenparametern verarbeitet (desinfiziert, gelöscht, in die Quarantäne verschoben).

EIN- UND AUSGABEPORT

Wird in Mikroprozessoren (z.B. Intel) beim Datenaustausch mit der Hardware verwendet. Der Ein- und Ausgabeport wird einem bestimmten Gerät zugeordnet und erlaubt es den Programmen, zum Datenaustausch darauf zuzugreifen.

E-MAIL LÖSCHEN

Verarbeitungsmethode für eine E-Mail, die Spam-Merkmale aufweist. Dabei wird die Nachricht physikalisch gelöscht. Diese Methode wird für E-Mails empfohlen, die eindeutig als Spam gelten. Vor dem Löschen einer Nachricht, wird ihre Kopie im Backup gespeichert (wenn diese Funktion nicht deaktiviert wurde).

EMPFOHLENE STUFE

Sicherheitsstufe, deren Funktionsparameter von Kaspersky Lab empfohlen werden und die einen optimalen Schutz Ihres Computers gewährleistet. Diese Stufe wird in der Grundeinstellung verwendet.

FEHLALARM

Situation, in der ein virenfreies Objekt von der Kaspersky-Lab-Anwendung als infiziert eingestuft wird, weil sein Code Ähnlichkeit mit einem Virus aufweist.

GEFÄHRLICHES OBJEKT

Objekt, in dem sich ein Virus befindet. Es wird davor gewarnt, mit solchen Objekten zu arbeiten, weil dies zur Infektion des Computers führen kann. Beim Fund eines infizierten Objekts wird empfohlen, das Objekt mit Hilfe des Kaspersky-Lab-Programms zu desinfizieren oder, falls die Desinfektion nicht möglich ist, es zu löschen.

GEPACKTE DATEI

Archivdatei, die ein Extrahierprogramm und für das Betriebssystem bestimmte Extrahierbefehle enthält.

GÜLTIGKEITSDAUER DER LIZENZ

Zeitraum, für den Sie berechtigt sind, das Kaspersky-Lab-Programm mit allen Funktionen zu nutzen. Die Gültigkeitsdauer der Lizenz beträgt in der Regel ein Kalenderjahr ab der Installation der Lizenz. Wenn die Gültigkeitsdauer der Lizenz abgelaufen ist, wird die Funktionalität des Programms eingeschränkt: Das Update der Datenbanken ist nicht mehr verfügbar.

HARDWARE-PORT

Eingang an einem Hardware-Element des Computers, an den ein Kabel oder ein Stecker angeschlossen werden kann (LPT-Port, serieller Port, USB).

HEURISTISCHE ANALYSE

Technologie zum Erkennen von Bedrohungen, die sich nicht mit Hilfe der Datenbanken von Anti-Virus identifizieren lassen. Es wird erlaubt, Objekte zu finden, die verdächtig sind, durch einen unbekannten Virus oder eine neue Modifikation eines bekannten Virus infizierte zu sein.

Mit Hilfe der heuristischen Analyse werden bis zu 92 % der neuen Bedrohungen erkannt. Dieser Mechanismus ist sehr effektiv und führt nur selten zu einem Fehlalarm.

Dateien, die mit Hilfe der heuristischen Analyse gefunden werden, nennt man verdächtig.

ICHECKER-TECHNOLOGIE

Diese Technologie erlaubt eine Erhöhung der Untersuchungsgeschwindigkeit. Dabei werden jene Objekte von der Untersuchung ausgeschlossen, die seit dem vorherigen Scannen nicht verändert wurden, wobei vorausgesetzt wird, dass die Untersuchungsparameter (Antiviren-Datenbanken und Einstellungen) gleich geblieben sind. Informationen darüber werden einer speziellen Datenbank aufgezeichnet. Die Technologie wird sowohl für den Echtzeitschutz als auch für den Scan auf Befehl verwendet.

Wurde beispielsweise eine Archivdatei vom Programm untersucht und ihr wurde der Status *virenfrei* zugewiesen. Dann wird das Archiv von der folgenden Untersuchung ausgeschlossen, wenn es nicht verändert wurde und die Untersuchungsparameter gleich geblieben sind. Wenn seit der letzten Untersuchung die Zusammensetzung des Archivs durch Hinzufügen eines neuen Objekts verändert wurde, die Untersuchungsparameter geändert oder die Programm-Datenbanken aktualisiert wurden, wird das Archiv erneut untersucht.

Einschränkungen der Technologie **iChecker**:

- Die Technologie funktioniert nicht mit großen Dateien, da die Untersuchung der gesamten Datei in diesem Fall weniger Zeit beansprucht, als zu ermitteln, ob sie seit der letzten Untersuchung verändert wurde.

- Die Technologie unterstützt eine begrenzte Anzahl von Formaten (**exe, dll, lnk, ttf, inf, sys, com, chm, zip, rar**).

INDIKATOR FÜR EINE VIRENEPIDEMIE

Vorlage, auf der eine Benachrichtigung über den drohenden Ausbruch einer Virenepidemie beruht. Der Indikator für eine Virenepidemie umfasst einige Einstellungen, die den Schwellenwert der Virenaktivität, die Verbreitungsart und den Meldungstext enthalten.

INFIZIERTES OBJEKT

Objekt, das schädlichen Code enthält: Bei der Untersuchung des Objekts wurde erkannt, dass ein Abschnitt des Objektcodes vollständig mit dem Code einer bekannten Bedrohung übereinstimmt. Die Kaspersky-Lab-Spezialisten warnen davor, mit solchen Objekten zu arbeiten, weil dies zur Infektion Ihres Computers führen kann.

INKOMPATIBLES PROGRAMM

Antiviren-Programm eines anderen Herstellers oder Programm von Kaspersky Lab, das nicht mit Kaspersky Administration Kit verwaltet werden kann.

INSTALLATION MIT STARTSZENARIO

Remote-Installation von Kaspersky-Lab-Programmen, mit der der Start der Aufgabe zur Remote-Installation mit einem konkreten Benutzerkonto (mehreren Benutzerkonten) verknüpft werden kann. Beim Anmelden des Benutzers in der Domäne wird versucht, das Programm auf dem Client-Computer zu installieren, auf dem sich der Benutzer angemeldet hat. Dieses Verfahren wird für die Installation von Programmen des Herstellers auf Computern empfohlen, die mit den Betriebssystemen Microsoft Windows 98 / Me laufen.

INTERCEPTOR

Subkomponente des Programms, die für die Untersuchung bestimmter Typen von E-Mails verantwortlich ist. Die Auswahl der zu installierenden Interceptoren ist davon abhängig, in welcher Rolle oder Rollenkombination das Programm eingesetzt werden soll.

INTERNETPROTOKOLL (IP)

Basisprotokoll für das Internet, das seit seiner Entwicklung im Jahre 1974 unverändert verwendet wird. Es führt die Grundoperationen bei der Datenübertragung von einem Computer auf einen anderen aus und dient als Basis für alle Protokolle höherer Ebenen wie TCP und UDP. Es kontrolliert die Verbindung und die Fehlerbehandlung. Technologien wie IPv4 und Maskierung ermöglichen es, umfangreiche Netzwerke hinter einer relativ geringen Anzahl von IP-Adressen zu verbergen (oder sogar hinter einer Adresse). Dadurch wird erlaubt, die Ansprüche des ständig expandierenden Internets unter Verwendung eines relativ begrenzten IPv4-Adressraums zu befriedigen.

KASPERSKY-LAB-UPDATESERVER

Liste der http- und ftp-Server von Kaspersky Lab, von denen das Programm die Updates für Datenbanken und Module auf Ihren Computer herunterlädt.

KONTROLLIERTES OBJEKT

Datei, die mit den Protokollen HTTP, FTP oder SMTP übertragen und von der Firewall zur Untersuchung durch das Kaspersky-Lab-Programm umgeleitet wird.

KOPFZEILE (HEADER)

Informationen, die am Anfang einer Datei oder E-Mail stehen und Basisdaten über Status und Verarbeitung der Datei (E-Mail) enthalten. Die Kopfzeile einer E-Mail enthält z.B. Angaben über Absender, Empfänger und Datum.

LAUFWERKSBOOTSEKTOR

Ein Bootsektor ist ein spezieller Sektor auf der Festplatte eines Computers, auf einer Diskette oder auf einem anderen Gerät zur Datenspeicherung. Er enthält Angaben über das Dateisystem des Datenträgers und ein Bootprogramm, das für den Start des Betriebssystems verantwortlich ist.

Laufwerksbootsektoren können von so genannten Bootviren infiziert werden. Die Kaspersky-Lab-Anwendung erlaubt es, Bootsektoren auf Viren zu untersuchen und infizierte Sektoren zu desinfizieren.

LISTE DER ZU UNTERSUCHENDEN WEBADRESSEN

Eine Liste der Masken und Webressourcen, die vom Kaspersky-Lab-Programm auf das Vorhandensein schädlicher Objekte unbedingt untersucht werden sollen.

LISTE MIT ERLAUBTEN ABSENDERN

(auch weiße Adressenliste)

Liste mit E-Mail-Adressen. Die von diesen Adressen eintreffenden Nachrichten werden nicht vom Kaspersky-Lab-Programm untersucht.

LISTE MIT ERLAUBTEN WEBADRESSEN

Eine Liste der Masken und Webressourcen, auf die der Zugriff vom Kaspersky-Lab-Programm nicht blockiert wird. Eine Adressenliste wird vom Benutzer bei der Programmkonfiguration erstellt.

LISTE MIT VERBOTENEN ABSENDERN

(auch schwarze Adressenliste)

Liste mit E-Mail-Adressen. Die von diesen Adressen eintreffenden Nachrichten werden vom Kaspersky-Lab-Programm ungeachtet ihres Inhalts blockiert.

LISTE MIT VERBOTENEN WEBADRESSEN

Eine Liste der Masken und Webressourcen, auf die der Zugriff vom Kaspersky-Lab-Programm blockiert wird. Eine Adressenliste wird vom Benutzer bei der Programmkonfiguration erstellt.

MAIL-DATENBANKEN

Datenbanken mit einem speziellem Format, in denen die auf Ihrem Computer gespeicherten E-Mails enthalten sind. Jede eingehende / ausgehende E-Mail wird nach dem Empfang / Senden in einer Mail-Datenbank gespeichert. Solche Datenbanken werden bei einer vollständigen Untersuchung des Computers untersucht.

Eingehende und ausgehende E-Mails werden im Augenblick des Empfangs und Sendens in Echtzeit auf Viren analysiert, wenn der Echtzeitschutz aktiviert ist.

MÖGLICHERWEISE INFIZIERTES OBJEKT

Objekt, dessen Code entweder den modifizierten Code eines bekannten Virus oder einen Code, der einem Virus gleicht, enthält, der Kaspersky Lab aber bisher nicht bekannt ist. Infizierte Dateien können mit Hilfe der heuristischen Analyse gefunden werden.

NETZWERKPORT

Parameter für die Protokolle TCP und UDP, der den Zweck von Datenpaketen im IP-Format definiert, die über ein Netzwerk auf einen Host übertragen werden. Er erlaubt unterschiedlichen auf einem Host ausgeführten Programmen,

unabhängig voneinander Daten zu empfangen. Jedes Programm verarbeitet die Daten, die auf einem bestimmten Port eintreffen (man sagt auch, ein Programm "hört" einen bestimmten Port).

Gewöhnlich sind häufig verwendeten Netzwerkprotokollen standardmäßige Portnummern zugeordnet (Webserver empfangen ihre Daten standardmäßig mit dem HTTP-Protokoll auf TCP-Port 80), obwohl ein Programm prinzipiell ein beliebiges Protokoll und einen beliebigen Port verwenden kann. Mögliche Werte: von 1 bis 65535.

OBJEKT BLOCKIEREN

Der Zugriff externer Programme auf ein Objekt wird verboten. Ein blockiertes Objekt kann nicht gelesen, ausgeführt, verändert oder gelöscht werden.

OBJEKTE IN DIE QUARANTÄNE VERSCHIEBEN

Verarbeitungsmethode für ein möglicherweise infiziertes Objekt. Dabei wird der Zugriff auf das Objekt gesperrt und das Objekt wird vom ursprünglichen Speicherort in den Quarantäneordner verschoben. Dort wird es in verschlüsselter Form gespeichert, um eine Infektion auszuschließen.

OBJEKT LÖSCHEN

Methode zur Objektbearbeitung, bei der das Objekt physikalisch von dem Ort gelöscht wird, an dem es vom Programm gefunden wurde (Festplatte, Ordner, Netzwerkressource). Diese Bearbeitungsmethode wird für gefährliche Objekte empfohlen, deren Desinfektion aus bestimmten Gründen nicht möglich ist.

OLE-OBJEKT

Objekt, das an eine andere Datei angehängt oder darin eingebettet ist. Das Kaspersky-Lab-Programm erlaubt es, OLE-Objekte auf das Vorhandensein von Viren zu untersuchen. Wenn Sie beispielsweise eine beliebige Tabelle aus Microsoft Office Excel in ein Dokument des Typs Microsoft Office Word einfügen, wird die Tabelle als OLE-Objekt untersucht.

POTENTIELL INFIZIERBARES OBJEKT

Ein Objekt das aufgrund seiner Struktur seines Formats von einem Angreifer als "Container" benutzt werden kann, um ein schädliches Objekt zu platzieren oder weiterzuverbreiten. In der Regel sind dies ausführbare Dateien mit Erweiterungen wie **com**, **exe**, **dll** usw. Das Risiko des Eindringens und der Aktivierung von schädlichem Code ist für solche Dateien relativ hoch.

PRIORITÄTSSTUFE FÜR EIN EREIGNIS

Merkmal eines Ereignisses, das bei der Arbeit der Kaspersky-Lab-Anwendung eingetreten ist. Es gibt vier Prioritätsstufen:

- **Kritisches Ereignis**.
- **Funktionsstörung**.
- **Warnung**.
- **Informative Meldung**.

Ereignisse des gleichen Typs können unterschiedliche Prioritätsstufen besitzen. Entscheidend ist die Situation, in der ein Ereignis eintritt.

PROGRAMM AKTIVIEREN

Der Aktivierungsvorgang für das Programm umfasst die Eingabe eines Aktivierungscodes und den anschließenden Download eines Schlüssels, mit dem das Programm prüft, ob Rechte für die Programmnutzung bestehen und welche Nutzungsdauer dafür gilt.

PROGRAMMEINSTELLUNGEN

Einstellungen für die Arbeit des Programms, die für alle Aufgabentypen gleich sind und sich auf das gesamte Programm beziehen, zum Beispiel Parameter für die Leistungsfähigkeit des Programms, Parameter für das Berichtswesen, Backup-Parameter.

PROGRAMM-MODULE

Dateien, die zum Lieferumfang von Kaspersky Lab gehören und für die Realisierung der wichtigsten Aufgaben zuständig sind. Jeder Art von Aufgaben, die das Programm realisiert (Echtzeitschutz, Virensuche, Update), entspricht ein eigenes ausführbares Modul. Wenn die vollständige Untersuchung Ihres Computers aus dem Hauptfenster gestartet wird, initiieren Sie den Start des Moduls für diese Aufgabe.

PROTOKOLL

Genau definierte und standardisierte Kombination von Regeln, die das Verhältnis zwischen Client und Server regulieren. Bekannte Protokolle und die entsprechenden Dienste sind z.B. HTTP (WWW), FTP und NNTP (News).

PROXYSERVER

Dienst in Computernetzwerken, mit dem Clients indirekte Anfragen an anderen Netzwerkservices richten können. Zunächst baut der Client eine Verbindung zu einem Proxyserver auf und fragt nach einer bestimmten Ressource (zum Beispiel nach einer Datei), die auf einem anderen Server liegt. Dann stellt der Proxyserver mit dem angegebenen Server eine Verbindung her und nimmt von ihm die Ressource entgegen oder schreibt die Ressource in seinen eigenen Cache (falls der Proxy einen Cache besitzt). In einigen Fällen kann die Client-Anfrage oder Server-Antwort vom Proxyserver zu bestimmten Zwecken geändert werden.

QUARANTÄNE

Ein bestimmter Ordner, in den alle möglicherweise infizierten Objekte verschoben werden, die bei der Untersuchung oder im Rahmen des Echtzeitschutzes gefunden werden.

RESERVELIZENZ

Lizenz, die für die Arbeit der Kaspersky-Lab-Anwendung hinzugefügt, aber nicht aktiviert wurde. Eine Reservelizenz wird aktiviert, wenn die Gültigkeit der aktiven Lizenz abläuft.

SCHLÜSSELDATEI

Datei mit der Endung **.key**, die Ihr persönlicher "Schlüssel" ist und für die Arbeit des Kaspersky-Lab-Programms erforderlich ist. Eine Schlüsseldatei ist im Lieferumfang des Produkts enthalten, wenn es bei einem Händler von Kaspersky Lab erworben wurde, oder sie wird Ihnen per E-Mail zugesandt, wenn das Produkt in einem Internet-Shop gekauft wurde.

SCHUTZSTATUS

Aktueller Schutzstatus, der das Sicherheitsniveau des Computers charakterisiert.

SCHWARZE LISTE FÜR SCHLÜSSELDATEIEN

Datenbank, die Informationen über von Kaspersky Lab gesperrte Schlüsseldateien enthält, deren Besitzer gegen die Bedingungen des Lizenzvertrags verstoßen haben, und über Schlüsseldateien, die zwar ausgegeben, aber nicht verkauft oder ersetzt wurden. Die Datei mit der schwarzen Liste ist für die Arbeit von Kaspersky-Lab-Programmen erforderlich. Die Datei wird gemeinsam mit den Datenbanken aktualisiert.

SCHWELLE FÜR VIRENAKTIVITÄT

Maximal zulässige Anzahl von Ereignissen eines bestimmten Typs innerhalb eines festgelegten Zeitraums, deren Überschreitung als erhöhte Virenaktivität und als Anzeichen eines Virenangriffs gilt. Dieser Wert besitzt insbesondere bei Viren-Epidemien große Bedeutung und erlaubt es dem Administrator, rechtzeitig auf drohende Virenangriffe zu reagieren.

SICHERHEITSSTUFE

Unter Sicherheitsstufe wird eine vordefinierte Auswahl von Parametern für die Arbeit einer Komponente verstanden.

SICHERUNGSKOPIEN

Bevor ein Desinfektionsversuch erfolgt oder die Datei gelöscht wird, legt die Anwendung eine Sicherungskopie an und speichert diese im Backup. Dadurch wird ermöglicht, die Datei bei Bedarf wiederherzustellen, um sie beispielsweise mit aktualisierten Datenbanken zu untersuchen.

SKRIPT

Ein kleines Computerprogramm oder ein unabhängiger Programmteil (Funktion), das/der in der Regel dazu dient, eine konkrete Aufgabe auszuführen. Meistens werden sie bei Programmen, die in Hypertext integriert sind, verwendet. Skripts werden beispielsweise gestartet, wenn Sie eine bestimmte Webseite öffnen.

Wenn der Echtzeitschutz aktiviert ist, überwacht die Anwendung den Start von Skripts, fängt sie ab und untersucht diese auf Viren. Abhängig von den Untersuchungsergebnissen können Sie die Ausführung eines Skripts verbieten oder erlauben.

SPAM

Unerwünschte massenhafte Versendung von E-Mails, die meistens Werbung enthalten.

SOCKS

Proxyserver-Protokoll, mit dem eine zweiseitige Verbindung zwischen Computern eines lokalen und externen Netzwerks realisiert werden kann.

SUBNETZMASKE

Die Subnetzmaske (auch Netzwerkmaske genannt) und die Netzwerkadresse definieren die Adressen der Computer, die zu einem Netzwerk gehören.

UNBEKANNTER VIRUS

Neuer Virus, über den noch keine Informationen in den Datenbanken vorhanden sind. Unbekannte Viren werden mit der heuristischen Analyse erkannt und erhalten den Status möglicherweise infiziert.

UNTERSUCHUNG DES DATENVERKEHRS

Untersuchung von Objekten, die mit beliebigen Protokollen übertragen werden (z.B. HTTP, FTP u.a.). Die Untersuchung erfolgt im Echtzeitmodus unter Verwendung der aktuellen (letzten) Datenbankversion.

UPDATE

Vorgang, bei dem vorhandene Dateien (Datenbanken oder Programm-Module) durch neue Dateien ersetzt bzw. neue Dateien hinzugefügt werden. Die neuen Dateien werden von den Kaspersky-Lab-Updateservern heruntergeladen.

UPDATEPAKET

Dateipaket, das der Softwareaktualisierung dient, aus dem Internet kopiert und auf Ihrem Computer installiert wird.

VERDÄCHTIGE E-MAIL

E-Mail, die sich nicht eindeutig als Spam einstufen lässt, bei deren Untersuchung sich aber ein Verdacht ergeben hat (z.B. bestimmte Arten von Massenmails und Werbenachrichten).

VERDÄCHTIGES OBJEKT

Objekt, dessen Code entweder den modifizierten Code eines bekannten Virus oder einen Code, der einem Virus gleicht, enthält, der Kaspersky Lab aber bisher nicht bekannt ist. Verdächtige Objekte werden unter Einsatz der heuristischen Analyse erkannt.

VERFÜGBARES UPDATE

Updatepaket für die Module einer Kaspersky-Lab-Anwendung, das dringende Updates, die über einen bestimmten Zeitraum gesammelt wurden, sowie Änderungen der Anwendungsarchitektur enthält.

VERTRAUENSWÜRDIGER PROZESS

Programmprozess, dessen Dateioperationen im Echtzeitschutz nicht von der Kaspersky-Lab-Anwendung kontrolliert werden. Das bedeutet, dass alle von einem vertrauenswürdigen Prozess gestarteten, geöffneten und gespeicherten Objekte nicht untersucht werden.

VIRENANGRIFF

Eine Reihe zielgerichteter Versuche, einen Computer mit einem Virus zu infizieren.

WIEDERHERSTELLUNG

Ein Originalobjekt wird aus der Quarantäne oder aus dem Backup entweder an den ursprünglichen Ort, an dem das Objekt gespeichert war, bevor es in die Quarantäne verschoben, desinfiziert oder gelöscht wurde, oder in einen benutzerdefinierten Ordner verschoben.

ZERTIFIKAT DES ADMINISTRATIONSSERVERS

Zertifikat, mit dem der Administrationsserver beim Herstellen einer Verbindung mit der Administrationskonsole und Datenaustausch mit den Client-Computern authentifiziert wird. Das Zertifikat des Administrationsservers wird bei Installation des Administrationsservers angelegt und im Unterordner **Cert** des Installtionsverzeichnisses gespeichert.

ENDBENUTZER-LIZENZVERTRAG FÜR DIE ERWORBENE KASPERSKY LAB SOFTWARE

WICHTIGER RECHTLICHER HINWEIS AN ALLE NUTZER: LESEN SIE FOLGENDE RECHTLICHE VEREINBARUNG SORGFÄLTIG DURCH, BEVOR SIE DIE SOFTWARE NUTZEN.

INDEM SIE IM LIZENZVERTRAG-FENSTER AUF DIE SCHALTFLÄCHE AKZEPTIEREN KLICKEN, ERKLÄREN SIE SICH MIT DER EINHALTUNG DER GESCHÄFTSBEDINGUNGEN DIESES VERTRAGS EINVERSTANDEN. **DIESE AKTION KONSTITUIERT EIN BEKENNTNIS IHRER SIGNATUR UND SIE STIMMEN DIESER VEREINBARUNG, UND DASS SIE EINE PARTEI DIESER VEREINBARUNG WERDEN, ZU UND ERKLÄREN SICH WEITERHIN EINVERSTANDEN, DASS DIESE VEREINBARUNG, WIE JEDWEDE ANDERE SCHRIFTLICHE, AUSGEHANDELTE UND DURCH SIE UNTERZEICHNETE VEREINBARUNG AUCH, VOLLSTRECKBAR IST.** SOLLTEN SIE MIT DEN GESCHÄFTSBEDINGUNGEN DIESER VEREINBARUNG NICHT EINVERSTANDEN SEIN, BEENDEN SIE DIE INSTALLATION DER SOFTWARE BZW. INSTALLIEREN SIE SIE NICHT.

NACHDEM SIE IM LIZENZVERTRAG-FENSTER AUF DIE SCHALTFLÄCHE AKZEPTIEREN GEKLICKT HABEN, SIND SIE BERECHTIGT, DIE SOFTWARE IM EINKLANG MIT DEN GESCHÄFTSBEDINGUNGEN DIESER VEREINBARUNG ZU NUTZEN.

1. Definitionen

1.1. **Software** bezeichnet Software, Benutzerhandbücher, zugehörige erläuternde oder sonstige Materialien, und zwar einschließlich jedweder Updates.

1.2. **Rechtsinhaber** (Inhaber aller Rechte an der Software, ob exklusiv oder anderweitig) bezeichnet Kaspersky Lab ZAO, ein gemäß den Gesetzen der Russischen Föderation amtlich eingetragenes Unternehmen.

1.3. **Computer** bezeichnet/bezeichnen Hardware, einschließlich von PCs, Laptops, Workstations, PDAs, Smart Phones, tragbaren oder sonstigen elektronischen Geräten, für welche die Software konzipiert war und auf denen die Software installiert werden wird.

1.4. **Endnutzer (Sie)** bezeichnet eine bzw. mehrere Personen, die die Software in eigenem Namen installieren oder nutzen, oder die eine Software-Kopie rechtmäßig nutzt/nutzen, oder, falls die Software im Namen einer Organisation heruntergeladen oder installiert wurde, wie etwa einem Arbeitgeber, bezeichnet der Begriff *„Sie“* weiterhin jene Organisation, für die die Software heruntergeladen oder installiert wird, und es wird hiermit erklärt, dass eine solche Organisation die diese Vereinbarung akzeptierende Person autorisiert hat, dies in ihrem Namen zu tun. Im Sinne dieses Lizenzvertrags beinhaltet der Begriff *„Organisation“* ohne Einschränkungen jedwede Partnerschaft, GmbH, Gesellschaft, Vereinigung, Aktiengesellschaft, Treuhandgesellschaft, Gemeinschaftsunternehmen, Arbeitsorganisation, nicht eingetragene Organisation oder staatliche Behörde.

1.5. **Partner** bezeichnet Organisationen oder Personen, die die Software auf Grundlage eines Vertrags und einer mit dem Rechtsinhaber vereinbarten Lizenz vertreiben.

1.6. **Update(s)** bezeichnet/n alle Upgrades, Korrekturen, Patches, Erweiterungen, Reparaturen, Modifikationen, Kopien, Ergänzungen oder Wartungs-Softwarepakete usw.

2. Lizenzgewährung

2.1. Der Rechtsinhaber gewährt Ihnen hiermit eine nicht-ausschließliche Lizenz zur Speicherung, zum Laden, zur Installation, Ausführung und Darstellung (zur „Nutzung“) der Software auf einer festgelegten Anzahl von Computern zur Unterstützung des Schutzes Ihres Computers, auf dem die Software installiert ist, vor im Nutzerhandbuch beschriebenen Bedrohungen im Einklang mit den Geschäftsbedingungen dieses Vertrags (die „Lizenz“), und Sie erkennen diese Lizenz an:

Testversion. Sollten Sie eine Testversion der Software erhalten, heruntergeladen und/oder installiert haben und sollte Ihnen hiermit eine Evaluierungslizenz für die Software gewährt worden sein, dürfen Sie die Software ab dem Datum der ersten Installation nur zu Evaluierungszwecken verwenden, und zwar ausschließlich während der einzigen geltenden Evaluierungsperiode, außer wie anderweitig angegeben. Jegliche Nutzung der Software zu anderen Zwecken oder über die geltende Evaluierungsperiode hinaus ist strikt untersagt.

Software für mehrere Umgebungen; Mehrsprachige Software; Dual-Medien-Software; Mehrere Kopien; Softwarebündel. Wenn Sie verschiedene Versionen der Software oder verschiedene Sprachausgaben der Software verwenden, wenn Sie die Software auf mehreren Medien erhalten, wenn Sie anderweitig mehrere Kopien der Software erhalten oder wenn Sie die Software mit einer anderen Software gebündelt erhalten

sollten, entspricht die insgesamt zulässige Anzahl Ihrer Computer, auf denen alle Versionen der Software installiert sind, der Anzahl der Lizenzen, die Sie vom Rechtsinhaber bezogen haben, und jede erworbene Lizenz berechtigt Sie zur Installation und Nutzung der Software auf dieser Anzahl von Computern entsprechend den Festlegungen in den Klauseln 2.2 und 2.3, *außer die* Lizenzbedingungen sehen eine anderweitige Regelung vor.

2.2. Wenn die Software auf einem physischen Medium erworben wurde, haben Sie das Recht, die Software zum Schutz einer solchen Anzahl von Computern zu verwenden, die auf der Softwareverpackung festgelegt ist.

2.3. Wenn die Software über das Internet erworben wurde, haben Sie das Recht, die Software zum Schutz einer solchen Anzahl von Computern zu verwenden, die genannt wurde, als Sie die Lizenz für die Software gekauft haben.

2.4. Sie haben das Recht, eine Kopie der Software anzufertigen, und zwar ausschließlich zu Sicherungszwecken und nur, um die rechtmäßig in Ihrem Besitz befindliche Kopie zu ersetzen, sollte eine solche Kopie verloren gehen, zerstört oder unbrauchbar werden. Diese Sicherungskopie kann nicht zu anderen Zwecken verwendet werden und muss zerstört werden, wenn Sie das Recht verlieren, die Software zu nutzen oder wenn Ihre Lizenz abläuft oder aus irgendeinem Grund im Einklang mit der gültigen Gesetzgebung im Land Ihres Wohnsitzes oder in dem Land, in dem Sie die Software nutzen, gekündigt werden sollte. Sie können die nicht-exklusive Lizenz zur Nutzung der Software an andere Personen oder Rechtspersönlichkeiten innerhalb des Rahmens der Ihnen vom Rechtsinhaber gewährten Lizenz übertragen, vorausgesetzt, dass der Empfänger allen Geschäftsbedingungen dieses Vertrags zustimmt bzw. bejaht, Sie vollständig in der vom Rechtsinhaber gewährten Lizenz zu vertreten. In dem Fall, dass Sie die vom Rechtsinhaber gewährten Rechte zur Nutzung der Software vollständig übertragen, müssen Sie alle Kopien der Software, und zwar einschließlich der Sicherungskopie, zerstören. Wenn Sie Empfänger einer übertragenen Lizenz sind, müssen Sie zustimmen, alle Geschäftsbedingungen dieses Vertrags einzuhalten. Wenn Sie den Geschäftsbedingungen dieses Vertrags nicht vollständig zustimmen, dürfen Sie die Software nicht installieren und/oder verwenden. Sie stimmen als Empfänger einer übertragenen Lizenz weiterhin zu, dass Sie über keine zusätzlichen oder besseren Rechte verfügen, als der ursprüngliche Endnutzer, der die Software vom Rechtsinhaber erworben hat.

2.5. Ab dem Zeitpunkt der Aktivierung der Software (mit Ausnahme einer Testversion der Software) haben Sie das Recht, folgende Dienstleistungen für den auf der Softwareverpackung (falls Sie Software auf einem physischen Medium erworben haben) oder während des Kaufs (falls die Software über das Internet erworben wurde) festgelegten Zeitraum zu beziehen:

- Updates der Software über das Internet, wenn und wie der Rechtsinhaber diese auf seiner Webseite oder mittels anderer Online-Dienste veröffentlicht. Jedwede Updates, die Sie erhalten, werden Teil der Software und die Geschäftsbedingungen dieses Vertrags gelten für diese;
- Technische Unterstützung über das Internet sowie technische Unterstützung über die Telefon-Hotline.

3. Aktivierung und Zeitraum

3.1. Falls Sie Modifikationen an Ihrem Computer oder an der darauf installierten Software anderer Anbieter vornehmen, kann der Rechtsinhaber von Ihnen verlangen, die Aktivierung der Software zu wiederholen. Der Rechtsinhaber behält sich das Recht vor, jegliche Mittel und Verifizierungsverfahren zu nutzen, um die Gültigkeit der Lizenz und/oder die Rechtmäßigkeit einer Kopie der Software, die auf Ihrem Computer installiert und/oder genutzt wird, zu verifizieren.

3.2. Falls die Software auf einem physischen Medium erworben wurde, kann die Software nach Ihrer Annahme dieses Vertrags mit Beginn ab dem Zeitpunkt der Annahme dieses Vertrags für die auf der Verpackung bezeichnete Periode genutzt werden.

3.3. Falls die Software über das Internet erworben wurde, kann die Software nach Ihrer Annahme dieses Vertrags für die während des Kaufs bezeichnete Zeitdauer genutzt werden.

3.4. Sie haben das Recht, eine Testversion der Software zu nutzen, und zwar gemäß der Festlegung in Klausel 2.1 und ohne jedwede Gebühr für die einzelne geltende Evaluierungsperiode ab dem Zeitpunkt der Aktivierung der Software im Einklang mit diesem Vertrag, *und zwar unter der Bedingung, dass* die Testversion Ihnen nicht das Recht auf Updates und technische Unterstützung über das Internet und technische Unterstützung über die Telefon-Hotline einräumt.

3.5. Ihre Lizenz zur Nutzung der Software beschränkt sich auf den in den Klauseln 3.2 oder 3.3 (je nach Anwendbarkeit) bezeichneten Zeitraum. Die verbleibende Zeitdauer kann unter Verwendung der grafischen Nutzerschnittstelle der Software eingesehen werden.

3.6. Unbeschadet anderer Rechtsmittel laut Gesetz oder Billigkeitsrecht, zu denen der Rechtsinhaber im Falle eines Verstoßes gegen die Geschäftsbedingungen dieses Vertrags durch Sie berechtigt ist, ist der Rechtsinhaber jederzeit, ohne Sie benachrichtigen zu müssen, dazu berechtigt, diese Lizenz zur Nutzung der Software zu kündigen, und zwar ohne den Verkaufspreis oder einen Teil davon zurückzuerstatten.

3.7. Sie stimmen zu, dass Sie bei der Nutzung der Software sowie bei der Verwendung jedweder Berichte oder Informationen, die sich als Ergebnis der Nutzung der Software ableiten, alle geltenden internationalen, nationalen, staatlichen, regionalen und lokalen Gesetze sowie gesetzlichen Bestimmungen, einschließlich (und ohne Beschränkung) Datenschutz-, Urheber-, Exportkontroll- und Verfassungsrecht, einhalten werden.

3.8. Außer wenn anderweitig hierin festgelegt, dürfen Sie keines der Rechte, die Ihnen unter diesem Vertrag gewährt werden, bzw. keine Ihrer hieraus entstehenden Pflichten übertragen oder abtreten.

4. Technische Unterstützung

Die in Klausel 2.5 dieses Vertrags erläuterte technische Unterstützung wird Ihnen gewährt, wenn das neueste Update der Software installiert wird (außer im Fall einer Testversion der Software).

5. Sammeln von Informationen

5.1. Durch Zustimmung zu den Geschäftsbedingungen dieses Vertrags haben Sie eingewilligt, dem Rechtsinhaber Informationen über die ausführbaren Dateien und ihre Prüfsummen zur Verfügung zu stellen, um Ihr Sicherheits-Schutzniveau zu verbessern.

5.2. Um das Sicherheitsbewusstsein bezüglich neuer Bedrohungen und deren Quellen zu verbessern, bzw. um Ihr Sicherheits-Schutzniveau zu verbessern, ist der Rechtsinhaber ausdrücklich berechtigt, mit Ihrer Zustimmung, die ausdrücklich in der Kaspersky Security Network Datenerfassungserklärung bestätigt wurde, derartige Informationen zu empfangen. Sie können den Kaspersky Security Network Service während der Installation deaktivieren. Sie können ebenfalls jederzeit auf der Softwareoptionsseite den Kaspersky Security Network Service aktivieren und deaktivieren.

Sie bestätigen und erkennen weiterhin an, dass jedwede Informationen, die vom Rechtsinhaber erfasst werden, zum Zweck der Verfolgung und Veröffentlichung von Sicherheitsrisikotrends verwendet werden können, und zwar nach freiem Ermessen des Rechtsinhabers.

5.3. Die Software verarbeitet keine personenbezogenen Daten und kombiniert keine Verarbeitungsdaten und persönlichen Informationen.

5.4. Sollten Sie nicht wünschen, dass die von der Software gesammelten Informationen an den Rechtsinhaber geschickt werden, sollten Sie den Kaspersky Security Network Service nicht aktivieren und/oder deaktivieren.

6. Beschränkungen

6.1. Sie werden die Software nicht emulieren, klonen, vermieten, verleihen, leasen, verkaufen, modifizieren, dekompilieren oder zurückentwickeln oder disassemblieren oder Arbeiten auf Grundlage der Software oder eines Teils davon ableiten, jedoch mit der einzigen Ausnahme eines Ihnen durch geltende Gesetzgebung gewährten Rechts, von dem keine Rücktretung möglich ist, und Sie werden in keiner anderen Form irgendeinen Teil der Software in menschlich lesbare Form umwandeln oder die lizenzierte Software oder irgendeine Teilmenge der lizenzierten Software übertragen, noch irgendeiner Drittpartei gestatten, dies zu tun, außer im Umfang vorangegangener Einschränkungen, die ausdrücklich durch geltendes Recht untersagt sind. Weder Binärcode noch Quellcode der Software dürfen verwendet oder zurückentwickelt werden, um den Programmalgorithmus, der proprietär ist, wiederherzustellen. Alle Rechte, die nicht ausdrücklich hierin gewährt werden, verbleiben beim Rechtsinhaber und/oder dessen Zulieferern, je nachdem, was zutrifft. Jegliche derartige nicht autorisierte Nutzung der Software kann zur sofortigen und automatischen Kündigung dieses Vertrags sowie der hierunter gewährten Lizenz und zu Ihrer straf- und/oder zivilrechtlichen Verfolgung führen.

6.2. Sie werden die Rechte zur Nutzung der Software nicht an eine Drittpartei übertragen, außer entsprechend der Festlegung in Klausel 2.4 dieses Vertrags.

6.3. Sie werden den Aktivierungscode und/oder die Lizenzschlüssel-Datei keinen Drittparteien verfügbar machen oder Drittparteien Zugang zum Aktivierungscode und/oder zum Lizenzschlüssel gewähren. Aktivierungscode und/oder Lizenzschlüssel werden/wird als vertrauliche Daten des Rechtsinhabers betrachtet, und Sie werden angemessene Sorgfalt zum Schutz der Vertraulichkeit des Aktivierungscodes und/oder des Lizenzschlüssels walten lassen, sofern Sie den Aktivierungscode und/oder den Lizenzschlüssel entsprechend der Festlegung in Klausel 2.4 dieses Vertrags an Drittparteien übertragen dürfen.

6.4. Sie werden die Software nicht an eine Drittpartei vermieten, verleasen oder verleihen.

6.5. Sie werden die Software nicht zur Erstellung von Daten oder Software verwenden, die zur Feststellung, zum Sperren oder zur Handhabung von Bedrohungen, wie im Nutzerhandbuch beschrieben, genutzt werden.

6.6. Der Rechtsinhaber hat das Recht, die Schlüsseldatei zu blockieren oder Ihre Lizenz zu kündigen, falls Sie gegen irgendwelche Geschäftsbedingungen dieses Vertrags verstoßen, und zwar ohne irgendeine Rückerstattung an Sie.

6.7. Falls Sie die Testversion der Software verwenden, sind Sie nicht berechtigt, technische Unterstützung, wie in Klausel 4 dieses Vertrags festgelegt, zu erhalten, und Sie sind ebenfalls nicht berechtigt, die Lizenz oder die Rechte zur Nutzung der Software an irgendeine Drittpartei zu übertragen.

7. Eingeschränkte Garantie und Haftungsausschluss

7.1. Der Rechtsinhaber garantiert, dass die Software im Wesentlichen im Einklang mit den im Nutzerhandbuch dargelegten Spezifikationen und Beschreibungen funktionieren wird, *jedoch vorausgesetzt,* dass eine solche eingeschränkte Garantie nicht für Folgendes gilt: (w) Mängel Ihres Computers und zugehörigen Verstoß, wofür der Rechtsinhaber ausdrücklich jedwede Gewährleistungsverantwortung ablehnt; (x) Funktionsstörungen, Defekte oder Ausfälle, resultierend aus falscher Verwendung, Missbrauch, Unfall, Nachlässigkeit, unsachgemäßer/m Installation, Betrieb oder Wartung, Diebstahl, Vandalismus, höherer Gewalt, terroristischen Akten, Stromausfällen oder -schwankungen, Unglück, Veränderung, nicht zulässiger Modifikation oder Reparaturen durch eine Partei außer dem Rechtsinhaber oder Maßnahmen einer sonstigen Drittpartei oder Aktionen ihrerseits, oder Ursachen außerhalb der Kontrolle des Rechtsinhabers; (y) jedweder Defekt, der dem Rechtsinhaber nicht durch Sie bekannt gemacht wird, sobald dies nach dem ersten Auftreten des Defekts möglich ist; und (z) Inkompatibilität, verursacht durch Hardware- und/oder Software-Komponenten, die auf Ihrem Computer installiert sind.

7.2. Sie bestätigen, akzeptieren und erkennen an, dass keine Software frei von Fehlern ist, und Sie sind angehalten, den Computer mit einer für Sie geeigneten Häufigkeit und Beständigkeit zu sichern.

7.3. Der Rechtsinhaber gibt keine Garantie, dass die Software im Fall von Verstößen gegen die Bedingungen, wie im Nutzerhandbuch oder in diesem Vertrag beschrieben, einwandfrei funktionieren wird.

7.4. Der Rechtsinhaber garantiert nicht, dass die Software einwandfrei funktionieren wird, wenn Sie nicht regelmäßig, wie in Klausel 2.5 dieses Vertrags erläutert, Updates herunterladen.

7.5. Der Rechtsinhaber garantiert keinen Schutz vor im Nutzerhandbuch beschriebenen Bedrohungen nach Ablauf der in Klausel 3.2 oder 3.3 dieses Vertrags bezeichneten Periode oder nachdem die Lizenz zur Nutzung der Software aus irgendeinem Grund gekündigt wurde.

7.6. DIE SOFTWARE WIRD OHNE MÄNGELGEWÄHR BEREITGESTELLT UND DER RECHTSINHABER GIBT KEINE ZUSICHERUNG UND KEINE GEWÄHRLEISTUNG IN BEZUG AUF IHRE NUTZUNG ODER LEISTUNG. DER RECHTSINHABER UND SEINE PARTNER GEWÄHREN AUßER DEN GARANTIEN, ZUSICHERUNGEN, BESTIMMUNGEN ODER BEDINGUNGEN, DIE DURCH GELTENDES RECHT NICHT AUSGESCHLOSSEN ODER BESCHRÄNKT WERDEN KÖNNEN, KEINE GARANTIEN, ZUSICHERUNGEN, BESTIMMUNGEN ODER BEDINGUNGEN (AUSDRÜCKLICHER ODER STILLSCHWEIGENDER NATUR, DIE ENTWEDER AUS EINER GESCHÄFTSBEZIEHUNG ODER EINEM HANDELSBRAUCH ENTSTEHEN BZW. AUS GESETZLICHEN, GEWOHNHEITSRECHTLICHTEN ODER ANDEREN VORSCHRIFTEN ABGELEITET WERDEN) HINSICHTLICH JEDWEDER ANGELEGENHEIT, EINSCHLIEßLICH (OHNE EINSCHRÄNKUNG) VON NICHTVERLETZUNG VON RECHTEN DRITTER, MARKTGÄNGIGKEIT, BEFRIEDIGENDE QUALITÄT, INTEGRIERUNG ODER BRAUCHBARKEIT FÜR EINEN BESTIMMTEN ZWECK. SIE TRAGEN DAS GESAMTE STÖRUNGSRISIKO UND DAS GESAMTRISIKO HINSICHTLICH DER LEISTUNG UND VERANTWORTUNG FÜR DIE AUSWAHL DER SOFTWARE, UM IHRE VORGESEHENEN RESULTATE ZU ERZIELEN, UND FÜR DIE INSTALLATION SOWIE DIE NUTZUNG DER SOFTWARE UND DIE MIT IHR ERZIELTEN ERGEBNISSE. OHNE EINSCHRÄNKUNG DER VORANGEGANGENEN BESTIMMUNGEN MACHT DER RECHTSINHABER KEINE ZUSICHERUNGEN UND GIBT KEINE GEWÄHRLEISTUNG, DASS DIE SOFTWARE FEHLERFREI ODER FREI VON UNTERBRECHUNGEN ODER SONSTIGEN STÖRUNGEN IST ODER DASS DIE SOFTWARE JEDWEDE ODER ALL IHRE ANFORDERUNGEN ERFÜLLEN WIRD, UNGEACHTET DESSEN, OB GEGENÜBER DEM RECHTSINHABER OFFEN GELEGT ODER NICHT.

8. Haftungsausschluss und Haftungsbeschränkungen

INSOWEIT GESETZLICH STATTHAFT, SIND DER RECHTSINHABER UND SEINE PARTNER UNTER KEINEN UMSTÄNDEN HAFTBAR FÜR JEDWEDE SPEZIELLEN ODER BEILÄUFIGEN SCHÄDEN, STRAFZUSCHLAG ZUM SCHADENERSATZ, INDIREKTE ODER FOLGESCHÄDEN (EINSCHLIEßLICH UND NICHT BESCHRÄNKT AUF SCHÄDEN AUS VERLUST VON GEWINN ODER VERTRAULICHEN ODER SONSTIGEN INFORMATIONEN, FÜR GESCHÄFTSUNTERBRECHUNG, FÜR VERLUST VON PRIVATSPHÄRE, KORRUPTION, BESCHÄDIGUNG UND VERLUST VON DATEN ODER PROGRAMMEN, FÜR VERSÄUMNIS EINER PFLICHTERFÜLLUNG, EINSCHLIEßLICH JEDWEDER GESETZLICHER PFLICHTEN, TREUEPFLICHT ODER PFLICHT ZUR WAHRUNG ANGEMESSENER SORGFALT, FÜR NACHLÄSSIGKEIT, FÜR WIRTSCHAFTLICHEN VERLUST UND FÜR FINANZIELLEN ODER JEDWEDEN SONSTIGEN VERLUST), DIE AUS ODER AUF IRGENDEINE WEISE IM ZUSAMMENHANG MIT DER NUTZUNG ODER UNMÖGLICHKEIT DER NUTZUNG DER SOFTWARE, DER BEREITSTELLUNG ODER DEM VERSÄUMNIS DER BEREITSTELLUNG TECHNISCHER UNTERSTÜTZUNG ODER SONSTIGER DIENSTLEISTUNGEN, INFORMATIONEN, SOFTWARE UND ZUGEHÖRIGEM INHALT MITTELS DER SOFTWARE RESULTIEREN, ODER SICH ANDERWEITIG AUS DER NUTZUNG DER SOFTWARE ODER ANDERWEITIG UNTER BZW. IM ZUSAMMENHANG MIT EINER BESTIMMUNG DIESES VERTRAGS ERGEBEN, ODER DIE FOLGE EINES VERTRAGSBRUCHS ODER UNERLAUBTER HANDLUNG (EINSCHLIEßLICH NACHLÄSSIGKEIT, FALSCHANGABE,

JEDWEDER STRIKTEN HAFTUNGSVERPFLICHTUNG ODER -PFLICHT), ODER EINER VERLETZUNG GESETZLICHER PFLICHTEN ODER DER GEWÄHRLEISTUNG DES RECHTSINHABERS ODER EINES SEINER PARTNER SIND, UND ZWAR AUCH DANN NICHT, WENN DER RECHTSINHABER ODER EINER SEINER PARTNER BEZÜGLICH DER MÖGLICHKEIT SOLCHER SCHÄDEN INFORMIERT WURDE.

SIE STIMMEN ZU, DASS IN DEM FALL, DASS DER RECHTSINHABER UND/ODER SEINE PARTNER HAFTBAR GEMACHT WERDEN/WIRD, DIE HAFTUNG DES RECHTSINHABERS UND/ODER SEINER PARTNER AUF DIE KOSTEN DER SOFTWARE BESCHRÄNKT IST. UNTER KEINEN UMSTÄNDEN WIRD DIE HAFTUNG DES RECHTSINHABERS UND/ODER SEINER PARTNER DIE FÜR DIE SOFTWARE ERSTATTETEN KOSTEN AN DEN RECHTSINHABER ODER DEN PARTNER ÜBERSTEIGEN (JE NACHDEM, WAS ZUTRIFFT).

NICHTS IN DIESEM VERTRAG SCHLIEßT EINEN ANSPRUCH AUFGRUND VON TOD UND PERSONENSCHADEN AUS ODER SCHRÄNKT DIESEN EIN. IN DEM FALL, DASS EIN HAFTUNGSAUSSCHLUSS, EIN AUSSCHLUSS ODER EINE EINSCHRÄNKUNG IN DIESEM VERTRAG AUFGRUND GELTENDEN RECHTS NICHT AUSGESCHLOSSEN ODER BESCHRÄNKT WERDEN KANN, WIRD NUR EIN SOLCHER HAFTUNGSAUSSCHLUSS, AUSSCHLUSS ODER EINE EINSCHRÄNKUNG NICHT FÜR SIE GELTEN, UND SIE SIND WEITERHIN AN JEDWEDE VERBLEIBENDEN HAFTUNGSAUSSCHLÜSSE, AUSSCHLÜSSE ODER EINSCHRÄNKUNGEN GEBUNDEN.

9. GNU und sonstige Drittpartei-Lizenzen

Die Software kann einige Softwareprogramme enthalten, die an den Nutzer unter der GPL (GNU General Public License) oder sonstigen vergleichbaren freien Softwarelizenzen lizenziert (oder unterlizenziert) sind und dem Nutzer neben anderen Rechten gestatten, bestimmte Programme oder Teile dieser Programme zu kopieren, zu modifizieren und weiter zu verbreiten und sich Zugang zum Quellcode zu verschaffen („Open Source Software“). Falls es solche Lizenzen erforderlich machen, dass für jedwede Software, die an jemanden in ausführbarem Binärformat geliefert wird, diesen Nutzern der Quellcode ebenfalls verfügbar gemacht wird, dann soll der Quellcode zur Verfügung gestellt werden, indem ein diesbezügliches Ersuchen an source@kaspersky.com gesendet wird. Falls irgendwelche Open Source Software-Lizenzen es erforderlich machen, dass der Rechtsinhaber Rechte zur Nutzung, zum Kopieren oder zur Änderung eines Open Source Software-Programms bereitstellt, welche umfassender sind, als die in diesem Vertrag gewährten Rechte, dann werden derartige Rechte Vorrang vor den hierin festgelegten Rechten und Einschränkungen haben.

10. Geistiges Eigentum

10.1 Sie stimmen zu, dass die Software sowie die Urheberschaft, Systeme, Ideen, Betriebsmethoden, Dokumentation und sonstige in der Software enthaltenen Informationen proprietäres geistiges Eigentum und/oder die wertvollen Geschäftsgeheimnisse des Rechtsinhabers oder seiner Partner sind und dass der Rechtsinhaber und seine Partner, je nachdem was zutrifft, durch das Zivil- und Strafrecht sowie durch Gesetze zum Urheberrecht, bezüglich Geschäftsgeheimnissen, Handelsmarken und Patenten der Russischen Föderation, der Europäischen Union und der Vereinigten Staaten sowie anderer Länder und internationaler Übereinkommen geschützt sind. Dieser Vertrag gewährt Ihnen keinerlei Rechte am geistigen Eigentum, einschließlich an jeglichen Handelsmarken und Servicemarken des Rechtsinhabers und/oder seiner Partner („Handelsmarken“). Sie dürfen die Handelsmarken nur so weit nutzen, um von der Software im Einklang mit der akzeptierten Handelsmarkenpraxis erstellte Druckausgaben zu identifizieren, einschließlich der Identifizierung des Namens des Besitzers der Handelsmarke. Eine solche Nutzung der Handelsmarke gibt Ihnen keinerlei Besitzrechte an dieser Handelsmarke. Der Rechtsinhaber und/oder seine Partner besitzen und behalten alle Rechte, Titel und Anteile an der Software, einschließlich (ohne jedwede Einschränkung) jedweden Fehlerkorrekturen, Erweiterungen, Updates oder sonstigen Modifikationen an der Software, ob durch den Rechtsinhaber oder eine beliebige Drittpartei vorgenommen, und allen Urheberrechten, Patenten, Rechten an Geschäftsgeheimnissen, Handelsmarken und sonstigem geistigen Eigentum daran. Ihr Besitz, die Installation oder Nutzung der Software lässt den Titel am geistigen Eigentum an der Software nicht auf Sie übergehen, und Sie erwerben keinerlei Rechte an der Software, außer jene ausdrücklich in diesem Vertrag dargelegten. Alle hierunter erstellten Kopien der Software müssen dieselben proprietären Informationen enthalten, die auf und in der Software erscheinen. Mit Ausnahme der hierin aufgeführten Bestimmungen gewährt Ihnen dieser Vertrag keine Rechte geistigen Eigentums an der Software und Sie bestätigen, dass diese unter diesem Vertrag gewährte Lizenz Ihnen gemäß den weiteren Festlegungen hierin ausschließlich das Recht auf eingeschränkte Nutzung unter den Geschäftsbedingungen dieses Vertrags gewährt. Der Rechtsinhaber behält sich alle Rechte vor, die Ihnen nicht ausdrücklich in diesem Vertrag gewährt wurden.

10.2 Sie bestätigen, dass der Quellcode, der Aktivierungscode und/oder die Lizenzschlüssel-Datei für die Software Eigentum des Rechtsinhabers sind und Geschäftsgeheimnisse des Rechtsinhabers konstituieren. Sie stimmen zu, den Quellcode der Software nicht zu modifizieren, abzuwandeln, zu übersetzen, zurückzuentwickeln, zu dekompilieren oder auf sonstige Weise zu versuchen, den Quellcode ausfindig zu machen.

10.3 Sie stimmen zu, die Software in keinster Weise zu modifizieren oder abzuändern. Sie dürfen die Urheberrechtshinweise oder sonstige proprietäre Hinweise auf jedweden Kopien der Software nicht entfernen oder verändern.

11. Geltendes Recht; Schiedsverfahren

Dieser Vertrag unterliegt den Gesetzen der Russischen Föderation und wird nach diesen ausgelegt, und zwar ohne Bezug auf gegenteilige gesetzliche Regelungen und Prinzipien. Dieser Vertrag wird nicht dem Übereinkommen der Vereinten Nationen über Verträge über den internationalen Warenverkauf unterliegen, dessen Anwendung ausschließlich ausgeschlossen wird. Jede Meinungsverschiedenheit, die aus den Bedingungen dieses Vertrags, deren Auslegung oder Anwendung oder einem Verstoß gegen diese resultiert, wird, außer falls durch unmittelbare Verhandlung beigelegt, durch das Gericht der internationalen Handelsschiedsgerichtsbarkeit bei der Industrie- und Handelskammer der Russischen Föderation in Moskau, in der Russischen Föderation, beigelegt. Jeder vom Schlichter abgegebene Schiedsspruch ist für die beteiligten Parteien endgültig und bindend und jedwedes Urteil bezüglich eines solchen Schiedsspruchs kann von jedem Gericht der zuständigen Jurisdiktion durchgesetzt werden. Nichts in diesem Abschnitt 11 wird eine Partei daran hindern, von einem Gericht der zuständigen Jurisdiktion rechtmäßige Entschädigung zu verlangen oder zu erhalten, sei es vor, während oder nach einem Schiedsverfahren.

12. Zeitraum für Rechtsverfolgung.

Von den Parteien dieses Vertrags kann keine Rechtsverfolgung, ungeachtet der Form, die sich aus Transaktionen unter diesem Vertrag ergibt, nach mehr als einem (1) Jahr nach dem Eintreten des Klagegrundes oder der Entdeckung dessen Eintritts ergriffen werden, außer, dass eine Rechtsverfolgung für Verletzung von Rechten geistigen Eigentums innerhalb des maximal geltenden gesetzlichen Zeitraums ergriffen wird.

13. Vollständigkeit der Vereinbarung, Salvatorische Klausel, kein Verzicht.

Dieser Vertrag stellt die Gesamtvereinbarung zwischen Ihnen und dem Rechtsinhaber dar und ersetzt jegliche sonstigen, vorherigen Vereinbarungen, Vorschläge, Kommunikation oder Ankündigung, ob mündlich oder schriftlich, in Bezug auf die Software oder den Gegenstand dieser Vereinbarung. Sie bestätigen, dass Sie diesen Vertrag gelesen haben, ihn verstehen und seinen Bedingungen zustimmen. Falls eine Bestimmung dieses Vertrags von einem Gericht der zuständigen Jurisdiktion insgesamt oder in Teilen als untauglich, ungültig oder aus welchen Gründen auch immer als nicht durchsetzbar angesehen wird, wird diese Bestimmung enger ausgelegt, damit sie rechtmäßig und durchsetzbar wird, und der Gesamtvertrag wird an diesem Umstand nicht scheitern, und die Ausgewogenheit des Vertrags bleibt weiterhin vollinhaltlich gültig und wirksam, so weit gesetzlich oder nach Billigkeitsrecht zulässig, während der ursprüngliche Inhalt weitest möglich beibehalten wird. Kein Verzicht auf eine hierin enthaltene Bestimmung oder Kondition ist gültig, außer in schriftlicher Form und durch Sie und einen autorisierten Vertreter des Rechtsinhabers unterzeichnet, vorausgesetzt, dass kein Verzicht einer Verletzung einer Bestimmung dieses Vertrags einen Verzicht eines vorherigen, gleichzeitigen oder Folgeverstoßes konstituiert. Nichtverfolgung oder fehlende Durchsetzung einer Bestimmung dieses Vertrags durch den Rechtsinhaber kann nicht als Verzicht auf diese Bestimmung oder dieses Recht geltend gemacht werden.

14. Kontaktinformationen.

Sollten Sie Fragen in Bezug auf diesen Vertrag haben oder sollten Sie wünschen, sich aus irgendeinem Grund mit dem Rechtsinhaber in Verbindung zu setzen, kontaktieren Sie bitte unsere Kundendienstabteilung unter:

Kaspersky Lab, 10/1 1st Volokolamsky Proezd
Moskau, 123060
Russische Föderation

Tel.: +7-495-797-8700
Fax: +7-495-645-7939

E-Mail: info@kaspersky.com

Webseite: www.kaspersky.com

© 2009 Kaspersky Lab ZAO. Alle Rechte vorbehalten. Die Software und jedwede begleitende Dokumentation unterliegen dem Urheberrecht bzw. dem Schutz durch Urheberrechtsgesetze und internationale Urheberrechtsabkommen sowie durch weitere Gesetze und Abkommen zum geistigen Eigentum.

KASPERSKY LAB

Kaspersky Lab wurde 1997 gegründet. Heute sind wir das bekannteste Unternehmen für Datenschutz-Software in Russland und bieten eine breite Palette an: Programmen zum Schutz vor Viren, unerwünschten E-Mails (Spam) und Hackerangriffen.

Kaspersky Lab ist ein international operierender Konzern. Die Zentrale befindet sich in Russland, es gibt Niederlassungen in Großbritannien, Frankreich, Deutschland, Japan, in den Benelux-Ländern, China, Polen, Rumänien und in den USA (Kalifornien). In Frankreich wurde eine neue Tochtergesellschaft gegründet, das Europäische Zentrum für Antiviren-Forschung. Unser Partnernetzwerk vereint weltweit mehr als 500 Unternehmen.

Kaspersky Lab – das sind heute mehr als tausend hoch qualifizierte Fachleute, von denen ein Dutzend MBA-Diplome und sechzehn einen Doktortitel besitzen. Die führenden Virusanalytiker von Kaspersky Lab gehören zur prestigeträchtigen Computer Anti-virus Researcher's Organization (CARO).

Das größte Kapital des Unternehmens sind das einzigartige Wissen und die Erfahren, die die Mitarbeiter im Laufe des mehr als vierzehnjährigen ununterbrochenen Kampfes gegen Viren gesammelt haben. Dank der ständigen Analyse von Virenaktivitäten können wir Tendenzen bei der Malware-Entwicklung vorhersagen und frühzeitig Benutzern einen zuverlässigen Schutz vor neuen Angriffen an die Hand geben. Dieser einzigartige Vorteil bildet die Basis der Produkte und Dienstleistungen von Kaspersky Lab. Wir sind unseren Wettbewerbern stets einen Schritt voraus und bieten unseren Kunden den besten Schutz.

Aufgrund der jahrelangen Tätigkeit wurde das Unternehmen zum führenden Entwickler von Technologien zum Schutz vor Viren. Kaspersky Lab hat als erstes Unternehmen viele moderne Standards für Antiviren-Software gesetzt. Die Basis-Software des Unternehmens heißt Kaspersky Anti-Virus® und sie sorgt für einen zuverlässigen Schutz aller Objekte vor Virenangriffen: Arbeitsstationen, Dateiserver, Mail-Systeme, Firewalls und Internet-Gateways sowie Taschencomputer. Bequeme Steuerelemente versetzen die Benutzer in die Lage, den Antivirenschutz von Computern und Unternehmensnetzwerken maximal zu automatisieren. Viele internationale Developer verwendeten in ihrer Software den Kernel von Kaspersky Anti-Virus, beispielsweise: Nokia ICG (USA), Aladdin (Israel), Sybari (USA), G Data (Deutschland), Deerfield (USA), Alt-N (USA), Microworld (Indien), BorderWare (Kanada).

Die Kunden von Kaspersky Lab kommen in den Genuss eines breiten Spektrums von Zusatzleistungen, die das störungsfreie Funktionieren der Erzeugnisse und die genaue Kompatibilität mit speziellen Business-Vorgaben garantieren. Wir projektieren, realisieren und begleiten Antiviren-Komplex-Lösungen von Unternehmen. Unsere Datenbanken werden stündlich aktualisiert. Wir haben für unsere Benutzer einen technischen Kundendienst in mehreren Sprachen eingerichtet.

Sollten Sie weitere Informationen wünschen, wenden Sie sich bitte an unsere Vertriebspartner oder direkt an Kaspersky Lab. Wir beraten Sie gern detailliert über das Telefon oder E-Mail. Auf Ihre Fragen bekommen Sie eine vollständige und erschöpfende Antwort.

Webseite von Kaspersky Lab:	http://www.kaspersky.de
Viren-Enzyklopädie:	http://www.viruslist.com/de/
Antiviren-Labor:	newvirus@kaspersky.com (nur zum Einsenden verdächtiger Objekte, die zuvor archiviert wurden) http://support.kaspersky.ru/virlab/helpdesk.html?LANG=de (für Fragen an die Virenanalytiker)
Webforum von Kaspersky Lab:	http://forum.kaspersky.com

SACHREGISTER

A

Algorithmus für die Arbeit
Mail-Anti-Virus ... 58
Algorithmus für die Arbeit
Datei-Anti-Virus ... 48
Algorithmus für die Arbeit
Web-Anti-Virus ... 65
Algorithmus für die Arbeit
IM-Anti-Virus ... 72
Algorithmus für die Arbeit
Programmkontrolle ... 75
Algorithmus für die Arbeit
Anti-Spam ... 104
Algorithmus für die Arbeit
Kindersicherung ... 127
Analyse von Netzwerkpaketen ... 195
Anti-Banner
Heuristische Analyse ... 123
Liste mit erlaubten Banneradressen ... 124
Liste mit verbotenen Banneradressen ... 125
Weiße Liste ... 124
Anti-Spam
Aggressivitätsstufe ... 109
Algorithmus für die Arbeit ... 104
Datenbank für Phishing-Webadressen ... 110
Erweiterung für Microsoft Office Outlook ... 119
Erweiterung für Microsoft Outlook Express ... 120
Erweiterung für The Bat! ... 121
Erweiterung für Thunderbird ... 122
Faktor für potentiellen Spam ... 104, 115
Filterung von E-Mails auf dem Server ... 117
Liste mit erlaubten Absendern ... 113
Liste mit erlaubten Absendern importieren ... 114
Liste mit erlaubten Phrasen ... 114
Liste mit verbotenen Absendern ... 111
Liste mit verbotenen Phrasen ... 112
Nachrichten für Microsoft Exchange Server ... 118
Spam-Faktor ... 104, 115
Standardparameter wiederherstellen ... 122
Training ... 106
zusätzliche Merkmale für die Spam-Filterung ... 116
Anti-Spam-Training
mit ausgehenden E-Mails. ... 107
mit Hilfe des Trainingsassistenten ... 106
mit Hilfe eines Mailprogramms ... 108
mit Hilfe von Berichten ... 109
Ausnahmen
Programmkontrolle ... 82

B

Backup ... 186
Berichte
Ereignistyp ... 201
Filterung ... 204
in Datei speichern ... 204
Komponente oder Aufgabe auswählen ... 199

Suche nach Ereignissen 205
BERICHTE 199
Beschränkungsstufe
Kindersicherung 129
Browser-Konfiguration 194

D

Datei-Anti-Virus
Arbeit anhalten 54, 55
Algorithmus für die Arbeit 48
Heuristische Analyse 51
Reaktion auf die Bedrohung 49
Schutzbereich 50
Sicherheitsstufe 49
Standardparameter wiederherstellen 56
Untersuchung optimieren 52
Untersuchung von zusammengesetzten Dateien 52
Untersuchungsmodus 53
Untersuchungstechnologie 53
Daten löschen
Sichere Umgebung 88
Datenbank für Phishing-Webadressen
Anti-Spam 110
IM-Anti-Virus 72
Web-Anti-Virus 67

E

Echtzeitschutz des Computers deaktivieren / aktivieren 159

F

Faktor für potentiellen Spam 115
Filterung von E-Mails auf dem Server
Anti-Spam 117
Firewall
Adressenbereich auswählen 95
Adressenbereich eines Netzwerks erweitern 90
Aktion auswählen, die von einer Regel ausgeführt werden soll 94
Assistent für neue Regeln 94
Firewall-Regel 92
Netzwerkstatus ändern 89
Paketregel 92
Parameter der Netzwerkverbindung 95
Regel für ein Programm 93
Firewall-Regel
Firewall 92

G

gemeinsamer Ordner
Sichere Umgebung 87

H

Heuristische Analyse
Anti-Banner 123
Datei-Anti-Virus 51
IM-Anti-Virus 73
Kindersicherung 134
Mail-Anti-Virus 62
Web-Anti-Virus 69

I

IM-Anti-Virus
Algorithmus für die Arbeit ... 72
Datenbank für Phishing-Webadressen ... 72
Heuristische Analyse ... 73
Schutzbereich ... 72
Infiziertes Objekt ... 263

K

Kaspersky Internet Security
beim Hochfahren des Betriebssystems starten ... 159
Kategorien der erkennbaren Bedrohungen ... 174
Kindersicherung
Aktion ... 134
Algorithmus für die Arbeit ... 127
Arbeit der Komponente ... 127
Beschränkungsstufe ... 129
Heuristische Analyse ... 134
Kategorien der verbotenen Webseiten ... 133
Profile ... 128
Profile wechseln ... 128
Schwarze Liste ... 132
Weiße Liste ... 130
Zeitbeschränkung für den Zugriff ... 134
Kontextmenü ... 42
Kontrolle des Zugriffs auf das Programm ... 160

L

Leistung des Computers ... 172
Lizenz ... 266
aktive ... 260
Schlüsseldatei herunterladen ... 266

M

Mail-Anti-Virus
Algorithmus für die Arbeit ... 58
Anlagenfilterung ... 62
Heuristische Analyse ... 62
Reaktion auf die Bedrohung ... 59
Schutzbereich ... 60
Sicherheitsstufe ... 58
Standardparameter wiederherstellen ... 63
Untersuchung von zusammengesetzten Dateien ... 62
Modul zur Link-Untersuchung
Web-Anti-Virus ... 68

N

Netzwerk
geschützte Verbindungen ... 179
kontrollierte Ports ... 178
Netzwerkmonitor ... 198
Notfall-CD ... 191

P

Paketregel
Firewall ... 92
Proaktiver Schutz
Gruppe mit vertrauenswürdigen Programmen ... 99
Kontrolle über Systembenutzerkonten ... 99

Liste der gefährlichen Aktivitäten ... 97
Regel für die Kontrolle einer gefährlichen Aktivität ... 98
Programmgruppen
Programmkontrolle ... 76
Programmhauptfenster ... 43
Programmkomponenten ... 18
Programmkontrolle
Algorithmus für die Arbeit ... 75
Ausnahmen ... 82
Programmgruppen ... 76
Rechte erben ... 75
Regel für ein Programm ändern ... 81
Regeln für die Programmkontrolle ... 79
Risikobewertung ... 76
Schutzbereich ... 77
Startfolge eines Programms ... 77
PROGRAMMOBERFLÄCHE ... 41

Q

Quarantäne und Backup ... 185
Quarantäne. ... 185

R

Reaktion auf die Bedrohung
Datei-Anti-Virus ... 49
Mail-Anti-Virus ... 59
Virensuche ... 140
Web-Anti-Virus ... 66
Rechte erben
Programmkontrolle ... 75
Regel für ein Programm
Firewall ... 93
Regel für ein Programm ändern
Programmkontrolle ... 81
Regeln für die Programmkontrolle
Programmkontrolle ... 79
Risikobewertung
Programmkontrolle ... 76

S

Schutz vor Netzwerkangriffen
Sperrdauer ... 100
Sperrung aufheben ... 100
Arten der erkennbaren Netzwerkangriffe ... 100
Schutzbereich
Datei-Anti-Virus ... 50
IM-Anti-Virus ... 72
Mail-Anti-Virus ... 60
Programmkontrolle ... 77
Web-Anti-Virus ... 67
Schutzmodus auswählen
Sichere Umgebung ... 86, 87
Selbstschutz für das Programm ... 170
Sichere Umgebung
Daten löschen ... 88
gemeinsamer Ordner ... 87
Schutzmodus auswählen ... 86, 87
Verknüpfung erstellen ... 85
Sicherheitsstufe
Datei-Anti-Virus ... 49

Mail-Anti-Virus ... 58
Web-Anti-Virus ... 66
Sicherungskopien ... 266
Spam-Faktor
Anti-Spam ... 104, 115
Standardparameter wiederherstellen
Anti-Spam ... 122
Datei-Anti-Virus ... 56
Mail-Anti-Virus ... 63
Startfolge eines Programms
Programmkontrolle ... 77
Suche nach Schwachstellen
Benutzerkonto ... 150
Liste der Untersuchungsobjekte ... 148
Zeitplan ... 149
Symbol im Infobereich der Taskleiste ... 41

U

Untersuchung
Aktion für ein gefundenes Objekt ... 140
Aufgabe starten ... 138
automatischer Start einer übersprungenen Aufgabe ... 145
Benutzerkonto ... 145
Sicherheitsstufe ... 140
Suche nach Schwachstellen ... 147
Typ der zu untersuchenden Objekte ... 141
Untersuchung optimieren ... 142
Untersuchung von zusammengesetzten Dateien ... 143
Untersuchungstechnologien ... 144
Zeitplan ... 145
Update
aus einem lokalen Ordner ... 155
Proxyserver verwenden ... 154
Regionsoptionen ... 154
Rollback zum vorherigen Update ... 153
Updatequelle ... 153

V

Verknüpfung erstellen
Sichere Umgebung ... 85
Vertrauenswürdige Zone
Regeln für Ausnahmen ... 175
Vertrauenswürdige Anwendungen ... 174
Virtuelle Tastatur ... 190

W

Web-Anti-Virus
Algorithmus für die Arbeit ... 65
Datenbank für Phishing-Webadressen ... 67
Heuristische Analyse ... 69
Modul zur Link-Untersuchung ... 68
Reaktion auf die Bedrohung ... 66
Schutzbereich ... 67
Sicherheitsstufe ... 66
Untersuchung optimieren ... 69
Wiederherstellung ... 268

Z

Zeitplan
Update ... 156
Virensuche ... 145